Internationale
Göttinger Reihe

RECHTSWISSENSCHAFTEN

Jacqueline Frinken

Die Verwendung von Daten aus vernetzten Fahrzeugen

unter besonderer Berücksichtigung des Umgangs mit solchen Daten durch den Arbeitgeber

Band 73

Cuvillier Verlag Göttingen
Internationaler wissenschaftlicher Fachverlag

Internationale Göttinger Reihe

Rechtswissenschaften

Band 73

Die Verwendung von Daten aus vernetzten Fahrzeugen

unter besonderer Berücksichtigung des Umgangs mit solchen Daten durch den Arbeitgeber

Dissertation

zur Erlangung des Grades eines

Doktors der Rechte

des Fachbereichs
Rechts- und Wirtschaftswissenschaften
der Johannes Gutenberg-Universität
Mainz

vorgelegt von

Jacqueline Frinken
Syndikusrechtsanwältin in Neuwied

2017

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der
Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet
über http://dnb.d-nb.de abrufbar.
1. Aufl. - Göttingen: Cuvillier, 2017
Zugl.: Mainz, Univ., Diss., 2017

Erstberichterstatter:
Prof. Dr. iur. Rolf Schwartmann

Zweitberichterstatter:
Prof. Dr. iur. Dieter Dörr

Tag der mündlichen Prüfung: 16. Februar 2017

Nonnenstieg 8, 37075 Göttingen
Telefon: 0551-54724-0
Telefax: 0551-54724-21
www.cuvillier.de

1. Auflage, 2017
Gedruckt auf umweltfreundlichem, säurefreiem Papier aus nachhaltiger Forstwirtschaft.

ISBN 978-3-7369-9486-7
eISBN 978-3-7369-8486-8

Meinen Eltern

Vorwort

Die vorliegende Arbeit wurde vom Fachbereich Rechts- und Wirtschaftswissenschaften der Johannes Gutenberg-Universität Mainz im Wintersemester 2016/2017 als Dissertation angenommen. Rechtsprechung und Literatur konnten bis Juni 2016 berücksichtigt werden.

Die Erstellung der Arbeit war für mich persönlich eine aufgrund der parallelen Berufstätigkeit sehr herausfordernde, aber dennoch überaus bereichernde Erfahrung. Die Arbeit entstand während meiner Teilzeittätigkeit in einer Kanzlei sowie ab September 2015 neben meiner Vollzeittätigkeit als Syndikusrechtsanwältin.

Thematisch gibt die Arbeit einen Überblick über die praxisrelevanten Bereiche des betrieblichen Einsatzes vernetzter Fahrzeuge und bietet eine Systematisierung der Problemkreise an.

Mein besonderer Dank gilt *Herrn Prof. Dr. Rolf Schwartmann* für die Betreuung meines Promotionsvorhabens und die Überlassung des hochinteressanten Themas. Weiter bedanke ich mich herzlich bei *Herrn Prof. Dr. Dieter Dörr* für die Bereitschaft und zügige Erstellung des Zweitgutachtens.

Für die motivierende und tatkräftige Unterstützung, die ich im Laufe des Promotionsvorhabens durch Wort und Tat erfahren habe, bedanke ich mich vielmals.

Auch für die mitunter nötigen Trostspenden und ermahnenden Worte bin ich aus tiefstem Herzen dankbar.

Mein größter Dank gilt an dieser Stelle meinen Eltern *Monika und Harald Frinken*, die mich während meines gesamten Studiums und insbesondere während meines Promotionsvorhabens unentwegt unterstützt haben. Ihr Verständnis und vorbehaltloser Rückhalt sind Zeichen dafür, dass sie immer bereit sind, alles Erdenkliche für meinen Bruder Marcel und mich zu tun.

Mainz, im Februar 2017 Jacqueline Frinken

Inhaltsverzeichnis

Abkürzungen

a.A.	andere Ansicht
aaO	am angegebenen Ort
ABl.	Amtsblatt
Abs.	Absatz
ABS	Antiblockiersystem
ACC	Adaptive Cruise Control
ADAC	Allgemeiner Deutscher Automobil-Club e.V.
a.E.	am Ende
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
a.F.	alte Fassung
AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
AO	Abgabenordnung
AöR	Archiv des öffentlichen Rechts
AP	Arbeitsrechtliche Praxis
API	Application Progamming Interface
App	Application Software
APuZ	Aus Politik und Zeitgeschichte
Arb-Aktuell	Arbeitsrecht aktuell
ArbG	Arbeitsgericht
Art.	Artikel
ASR	Antriebsschlupfregelung
ATZ	Automobiltechnische Zeitschrift
AU	Abgasuntersuchung
Aufl.	Auflage
AuR	Arbeit und Recht
Az.	Aktenzeichen
BayDSG	Bayerisches Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung
BayRS	Bayerische Rechtssammlung
BB	Der Betriebsberater
BbgDSG	Gesetz zum Schutz personenbezogener Daten im Land Brandenburg
BDSG	Bundesdatenschutzgesetz
BDSG-E	Entwurf des Bundesdatenschutzgesetzes
BeckRS	Beck-Rechtsprechung
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt

BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien
BKA	Bundeskriminalamt
BlnDSG	Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung
BMI	Bundesministerium des Inneren
BPersVG	Bundespersonalvertretungsgesetz
BR-Drs.	Bundesratsdrucksache
BremDSG	Bremisches Datenschutzgesetz
BremGBl	Gesetzblatt Bremen
bspw.	beispielsweise
BT-Drs.	Bundestagsdrucksache
BUS	Binary Unit System
bzw.	beziehungsweise
CAN	Control Area Network
CD	Compact Disk
CDU	Christlich Demokratische Union Deutschlands
CR	Computer und Recht
CSU	Christlich-Soziale Union in Bayern
DAB	Digital Audio Broadcast
DAR	Deutsches Autorecht
DAV	Deutsche Anwaltverein
DB	Der Betrieb
DEKRA	Deutscher Kraftfahrzeug-Überwachungs-Verein
DGB	Deutscher Gewerkschaftsbund
d.h.	das heißt
DIMDIV	Verordnung über das datenbankgestützte Informationssystem über Medizinprodukte des Deutschen Instituts für Medizinische Dokumentation und Information
DIW	Deutsches Institut für Wirtschaftsforschung e.V.
Drs.	Drucksache
DSG-LSA	Gesetz zum Schutz personenbezogener Daten der Bürger
DSG-MV	Datenschutzgesetz Mecklenburg-Vorpommern
DSG-NW	Datenschutzgesetz Nordrhein-Westfalen
DS-GVO	Datenschutz-Grundverordnung
DS-RL	Datenschutz-Richtlinie
dt.	deutsch
DuD	Datenschutz und Datensicherheit
eCall	Emergency Call
EDR	Event Data Recorder
EG	Europäische Gemeinschaft

EGV	Vertrag der Europäischen Gemeinschaft
EL	Ergänzungslieferung
ElGVG	Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz
EP	Europäisches Parlament
E-Privacy-RL	Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation
ESP	Elektronisches Stabilitätsprogramm
etc.	et cetera
EU	Europäische Union
EU-GRCH	Charta der Grundrechte der Europäischen Union
EURO 5/6 VO	Verordnung (EG) Nr. 715/2007 des Europäischen Parlaments und des Rates vom 20. Juni 2007 über die Typgenehmigung von Kraftfahrzeugen hinsichtlich der Emissionen von leichten Personenkraftwagen und Nutzfahrzeugen
EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
f.	folgende
FD-StrVR	Fachdienst Straßenverkehrsrecht
FeV	Fahrerlaubnisverordnung
ff.	fortfolgende
FIN	Fahrzeugidentifikationsnummer
Fn.	Fußnote
GG	Grundgesetz
GK-BetrVG	Gemeinschaftskommentar zum Betriebsverfassungsgesetz
GNSS	Global Navigation Satellite System
GPRS	General Packet Radio Service
GPS	Global Positioning System
GRUR Int	Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil
GSM	Global System for Mobile Communication
GVBl	Gesetz- und Verordnungsblatt
GVNW	Gesetz- und Verordnungsblatt für das Land Nordrhein-Westfalen
HDSG	Hessisches Datenschutzgesetz
HmbgDSG	Hamburgisches Datenschutzgesetz
HMI	Human Machine Interface
HUD	Head Up Display
ID	Identifikationsnummer
IMSI	International Mobile Subscriber Identity
ITS	Intelligent Transport System

iVm	in Verbindung mit
IVS	Intelligente Verkehrssysteme
IVSG	Gesetz über Intelligente Verkehrssysteme im Straßenverkehr und deren Schnittstellen zu anderen Verkehrsträgern
IVS-RL	Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern
JuS	Juristische Schulung
Kfz	Kraftfahrzeug
Km/h	Kilometer pro Stunde
KUG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie
LAG	Landesarbeitsgericht
LBS	Local Based Services
LCS	Lane Change Support
LDSG-BW	Landesdatenschutzgesetz Baden-Württemberg
LDSG-RP	Landesdatenschutzgesetz Rheinland-Pfalz
LDSG-SH	Landesdatenschutzgesetz Schleswig-Holstein
LDW	Lane Departure Warning
LfD	Landesbeauftragter für den Datenschutz
LG	Landgericht
LIN	Local Interconnect Network
Lit.	Litera
LKS	Lane Keeping Support
LKW	Lastkraftwagen
LPersVG	Landespersonalvertretungsgesetz
MDM	Mobilitäts Daten Marktplatz
MES	Mobile Einsatzsteuerung für die Außendienst-Tourenplanung
MMI	Man Machine Interface
MMR	MultiMedia und Recht
MOST	Media Oriented Systems Transport
MPU	Medizinisch-Psychologische Untersuchung
MSD	Minimum Set of Data
MüKo	Münchener Kommentar
NDSG	Niedersächsisches Datenschutzgesetz
NJOZ	Neue Juristische Online-Zeitschrift
NJW	Neue Juristische Wochenschrift
NJW-RR	Neue Juristische Wochenschrift Rechtsprechungs-Report

Nr.	Nummer
NStZ	Neue Zeitschrift für Strafrecht
NStZ-RR	Neue Zeitschrift für Strafrecht Rechtsprechungs-Report
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZA	Neue Zeitschrift für Arbeitsrecht
NZV	Neue Zeitschrift für Verkehrsrecht
OBD	On-Board-Diagnose
OBU	On-Board-Unit
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PDA	Personal Digital Assistent
PersV	Die Personalvertretung
PIN	Persönliche Identifikationsummer
POI	Point of Interest
RdA	Recht der Arbeit
RDS	Radio Data System
RDV	Recht der Datenverarbeitung
RFID	Radio-frequency Identification
RL-Bereitstellung-E	Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte
Rn.	Randnummer
RSU	Road Site Unit
S.	Seite
SächsDSG	Sächsisches Datenschutzgesetz
sCall	Service Call-System
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung
SDSG	Saarländisches Datenschutzgesetz
SGB	Sozialgesetzbuch
SIM	Subscriber Identity Module
simTD	Sichere Intelligente Mobilität – Testfeld Deutschland
SMS	Short Message Service
sog.	Sogenannt
SPD	Sozialdemokratische Partei Deutschlands
SprAuG	Sprecherausschussgesetz
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVZO	Straßenverkehrszulassungsordnung
SVR	Straßenverkehrsrecht

T	Tonne
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TFT	Thin-film transistor
ThürDSG	Thüringer Datenschutzgesetz
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
TMC	Traffic Message Channel
TMG	Telemediengesetz
TOP	Tagesordnungspunkt
u.a.	unter anderem
Überb	Überblick
UDS	Unfalldatenspeicher
UKW	Ultrakurzwelle
UN/ECE	Wirtschaftskommission für Europa der Vereinten Nationen
UrhG	Urheberrechtsgesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
v.	vom
VDA	Verband der Automobilindustrie
VG	Verwaltungsgericht
VGH	Verfassungsgerichtshof
vgl.	vergleiche
VGT	Verkehrsgerichtstag
VO	Verordnung
VW	Versicherungswirtschaft
WLAN	Wireless Local Area Network
WP	Working Paper
WÜ-StV	Wiener Übereinkommen vom 08. November 1968 über den Straßenverkehr
z.B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZfA	Zeitschrift für Arbeitsrecht
zfs	Zeitschrift für Schadensrecht
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik
Zit.	Zitiert
ZPO	Zivilprozessordnung

Kapitel 1: Einführung

Der mit dem Datenschutzrecht zu verwirklichende Persönlichkeitsschutz des Einzelnen wird in Zeiten rasant voranschreitender technischer Entwicklungen auf eine harte Probe gestellt. Die Technik hält immer mehr Einzug in sämtliche Lebensbereiche. Dabei schreitet die Entwicklung neuer technischer Geräte und Anwendungen derart schnell voran, dass es nahezu unmöglich erscheint, diese Entwicklungen zeitnah politisch wie auch rechtlich greifen und regulieren zu können. Reaktion statt Proaktion.

Auch bei dem der vorliegenden Untersuchung zugrundeliegenden Komplex technischen Fortschritts verhält es sich so. Die Liste der im Kraftfahrzeug entstehenden Daten ist lang.[1]

Der moderne Autofahrer möchte sein Auto nicht mehr nur als Fortbewegungsmittel einsetzen, sondern sein Smartphone und seine tragbaren Geräte nutzen, um sie mit dem Kraftfahrzeug zu vernetzen.[2] Mit der Entwicklung neuer Sensoren, Fahrerassistenzsysteme, mobiler Anwendungen und der Einführung von Elementen der Verkehrstelematik ist eine Vernetzung von Kraftfahrzeugen untereinander und mit der Straße bereits jetzt möglich. Die sog. Car to X-Kommunikation beschreibt das Phänomen, dass Kraftfahrzeuge in naher Zukunft untereinander kommunizieren sollen. Auch eine Kommunikation mit der Straße soll darüber ermöglicht werden. Vorwiegende Ziele sind dabei die Erhöhung der Verkehrssicherheit für alle Beteiligten sowie die Gewährleistung von noch mehr Fahrkomfort für den Nutzer eines Kraftfahrzeugs. Hindernisse und Unfälle sollen bereits einige Hundert Meter im Voraus dem Fahrer angezeigt werden. Auch der Einsatz von Ortungssystemen im Rahmen eines Beschäftigungsverhältnisses und im Flottenmanagement zieht weite Kreise. So hat beispielsweise ein Flottenbetreiber ein Interesse daran, durch Routenverfolgung die für ihn notwendige Einsatzplanung umzusetzen. Aber auch das Angebot an Telematik-Versicherungen steigt an. Dem Verbraucher wird angeboten, durch den Einbau einer Telematik-Box in seinem Fahrzeug und durch Auswertung der sich daraus ergebenden Score-Werte bei positivem Ergebnis eine Ersparnis der Versicherungsprämie erzielen zu können.

---

1 Vgl. http://www.car-it.com/heikle-datenstroeme-wem-gehoeren-die-daten-aus-dem-fahrzeug/id-0038906. Diese und alle folgenden Internetquellen wurden abgerufen am 11.07.2016.

2 So *Schwartmann/Ohr*, RDV 2015, S. 59–68 (59).

Zu kurz kommt bislang jedoch die Auseinandersetzung mit möglichen Gefahrenquellen und Missbrauchsgefahren, die sich aus der Vernetzung von Kraftfahrzeugen untereinander und mit mobilen Endgeräten ergeben können. Eine Fernschaltung und damit Fernsteuerung einzelner Kraftfahrzeuge von außen ist ebenso denkbar, wie die Schaffung eines gläsernen Autofahrers. Durch die Verwendung von Daten, die in den jeweiligen Sensoren im Kraftfahrzeug generiert werden, und deren Verknüpfung untereinander wird es greifbar, dadurch ein umfassendes Bewegungsprofil des Fahrers zu zeichnen, seine Interessen zu erkennen und darauf zu reagieren oder ihm ein etwaiges Fehlverhalten nachzuweisen.

Vernetzte Fahrzeuge sind dabei technisch wie rechtlich betrachtet nicht mehr nur Verkehrsmittel, sondern auch Quellen personenbezogener und nicht personenbezogener Daten, die über das Kraftfahrzeug an einen unbestimmten Kreis von Empfängern übermitteln werden können. Relevant wird dies insbesondere im Zusammenhang mit intelligenten Verkehrssystemen, Telekommunikations- und Telemediendiensten, IT-Sicherheitsrisiken, Drittlandexporten und in Bezug auf Beweismittel in Zivil- und Strafverfahren. Der Kreis der Empfänger ist nahezu undefinierbar. Auch die Auswirkungen, die die Kenntnis Dritter über die eigenen Daten haben, werden bisher verkannt. Für Aufsehen sorgte in diesem Zusammenhang eine Aussage des Marketing-Chefs von Ford, Jim Farley, die er jedoch – kaum ausgesprochen – zurücknehmen musste:

> *„Wir kennen jeden Autofahrer, der die Verkehrsregeln bricht. Und wir wissen, wo und wie jemand das tut.“*[3]

Dass dies jedoch verhindert werden muss, betonte Bundesjustiz- und Verbraucherschutzminister Heiko Maas bereits im Juli 2014:

> *„Was wir nicht wollen, ist der gläserne Autofahrer, für den Bewegungsprofile erstellt und Daten über den Fahrstil gesammelt werden.“*[4]

Auch die Ankündigung von Google und Apple, in den Markt für Betriebs- und Navigationssysteme in Automobilen einzusteigen und mit namhaften Herstellern zu kooperieren, wird zu weiteren Diskussionen in diesem Bereich führen.[5] Insbesondere wird die

---

3 Vgl. *Eicher*, ADAC Motorwelt (4/2014), S. 16–20 (17).

4 Vgl. http://www.cio.de/a/bundesjustizminister-fordert-datenschutz-im-auto,2962888.

5 Vgl. http://maertin-collegen.com/blog/datenschutz/automotive-und-datenschutz-problemzone-fahrzeugdaten/.

Schere zwischen dem gesellschaftliche Mehrwert sowie der Faszination für neue technische Möglichkeiten auf der einen und die kritische Beurteilung der mobilen Datenschleudern auf der anderen Seite größer werden.[6] Eines der Hauptprobleme ist jedoch weiterhin, dass im Hinblick auf nahezu alle technischen Daten nur die Hersteller Kenntnis darüber haben, welche Daten erhoben, gespeichert oder übermittelt werden:

> *„Die Hersteller sitzen auf den Daten und können damit machen, was sie wollen."*[7]

Die Reaktion auf die fortschreitenden technischen Neuerungen ist zwar bereits im Fluss. Ausreichender Schutz besteht allerdings bislang nicht. Die Gefahren, die sich für den Einzelnen aus der Zugriffsmöglichkeit auf seine Daten aus dem Kraftfahrzeug ergeben, sind zum jetzigen Zeitpunkt nicht umfänglich anhand der bestehenden gesetzlichen Regelungen einzufangen. Einigkeit besteht jedoch dahingehend, dass eine reibungslos funktionierende Kommunikation trotz verschiedener Techniksysteme der einzelnen Hersteller einer Standardisierung bedarf.[8]

Von Seiten der Rechtswissenschaftler ist das Verhältnis der Möglichkeiten und Risiken vernetzten und autonomen Fahrens zueinander zu bestimmen und gleichzeitig die aktuelle und zukünftig nötige Ausgestaltung der rechtlichen und politischen Rahmenbedingungen in Deutschland sowie international zu hinterfragen. Die Anpassung des rechtlichen Regelungsgefüges soll auf europäischer Ebene insbesondere durch den Erlass der Datenschutz-Grundverordnung erfolgen. Der Erlass derselben hat auch unmittelbare Auswirkungen auf die geplante Novelle des Bundesdatenschutzgesetzes in Bezug auf den Teilaspekt des Beschäftigtendatenschutzes, welche bereits über einige Legislaturperioden geplant, jedoch bislang nicht realisiert werden konnte. Im Hinblick auf die Einführung und Entwicklung intelligenter Verkehrssysteme wurde mittlerweile auf Grundlage der sog. IVS-Richtlinie[9] auf nationaler Ebene das sog. Intelligente Verkehrssysteme Gesetz (IVSG) erlassen. Die nationale Mitwirkung am europäischen Prozess wird

---

6 So *Kamps*, Internationales Verkehrswesen 2014, S. 18–19 (18).

7 So der Generalsekretär des Europäischen Automobil Clubs, Matthias Knobloch, vgl. http://www.wiwo.de/technologie/auto/vernetzte-fahrzeuge-konzerne-beginnen-autofahrer-zu-bevormunden/9647526-all.html.

8 Vgl.http://www.auto-motor-und-sport.de/news/vernetzte-autos-europa-beschliesst-kommunikationsstandards-8052692.html.

9 *Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern*, ABl. Nr. L 207 vom 06.08.2010, S. 1.

durch die Entwicklung des nationalen IVS-Aktionsplans *„Straße“* gewährleistet.[10] Ein erster Schritt zur Vernetzung von Kraftfahrzeugen mit straßenseitigen Einrichtungen, wie Ampelanlagen ist damit getan.

Im Zusammenhang mit der Verwendung von Daten aus vernetzten Fahrzeugen stellen sich neben den technischen auch vielfältige ethische wie rechtliche Fragen. Die wohl häufigste und am weitläufigsten diskutierte Frage ist dabei die Folgende:

„Wem gehören die Daten?“[11]

Besonders relevant ist die Frage, wem die Daten *„gehören“* oder ob sie überhaupt jemandem *„gehören“* können bzw. wem eine Zugriffsbefugnis auf die Daten zusteht, nicht nur aufgrund der vielfältigen Akteure bei der Verwendung von Daten aus Kraftfahrzeugen. Es stellt sich die Frage, ob Daten überhaupt eigentumsfähig sind oder ob hierfür nicht vielmehr auf den Datenträger an sich abzustellen ist und deshalb für die Daten an sich andere Zuordnungsrechte Anwendung finden müssen.

Wenn Daten erst einmal erhoben und gespeichert sind, wächst die Begehrlichkeit auf diese.[12] Neben Herstellern und Werkstätten besteht u.a. auch auf Seiten von Versicherern, Behörden und Flottenbetreibern ein Interesse an den Daten, die unter Umständen Aufschluss über ein relevantes Verhalten des Fahrers geben. So muss geklärt werden, wem an welchen Daten eine Zugriffsbefugnis zusteht und wer im datenschutzrechtlichen Sinne verantwortlich ist. Der Gefahr einer missbräuchlichen und unzulässigen Datenverwendung muss vor allem auch im Bereich des Beschäftigtendatenschutzes begegnet werden. Neben gesetzlichen Erlaubnistatbeständen kommt hier der Problematik der Freiwilligkeit einer vom Arbeitnehmer erteilten Einwilligung eine besondere Bedeutung zu.

---

10 Vgl. http://www.bmvi.de/SharedDocs/DE/Artikel/DG/ivs-im-strassenverkehr.html?linkToOverview=js.

11 Vgl. dazu beispielsweise nur http://www.verkehrswachtstiftung.de/news/wem-gehoeren-die-fahrzeugdaten.html; http://www.versicherungsbote.de/id/4813081/Telematik-Tarif-Kfz-Versicherung-ADAC-Kfz-Telematik/; http://www.car-it.com/rechtsfreier-raum-wem-gehoeren-die-daten-aus-dem-auto/id-0039081; http://www.morgenweb.de/nachrichten/vermischtes/wem-gehoren-fahrzeugdaten-1.1381526; vgl. auch *Bönninger*, zfs 2014 S. 184–189.

12 So der damalige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Peter Schaar bei einem ADAC-Fachgespräch am 28.09.2006 in München, vgl. http://www.bfdi.bund.de/DE/Infothek/Reden_Interviews/2006/GlaesernerAutofahrerUnterGeneralverdacht.html?nn=5217192.

Für die praktische Umsetzung der sich aus dem Regelungsgefüge des Datenschutzrechts ergebenden Rechte und Pflichten besteht die Schwierigkeit bisweilen darin, dass es dem Betroffenen nicht möglich ist zu wissen, welche Daten aus dem Kraftfahrzeug überhaupt anfallen oder verwendet werden. An der notwendigen Transparenz mangelt es erheblich. Den meisten Autofahrern wird nicht bewusst sein, welche Vielzahl an Informationen sie in das Kraftfahrzeug bringen und wie diese – auch gegen sie – verwendet werden könnten. Zunächst sieht ein Autofahrer als Verbraucher in den vielfältigen Angeboten und Diensten für sich lediglich die Vorteile einer mitunter vermeintlich kostenlosen Nutzung derselben. Dass die Nutzung jedoch oftmals an die Preisgabe von persönlichen Daten gekoppelt ist, fällt entweder erst gar nicht auf oder erscheint hinnehmbar, da auch im Hinblick auf den monetären Wert von persönlichen Daten bei den Einzelnen die notwendige Transparenz und deshalb auch die Kenntnis fehlen.

Das Ziel der Reformen des Datenschutzes muss es sein, dem gläsernen Menschen und insbesondere dem gläsernen Autofahrer entgegenzuwirken. Dies verlangt jedoch eine datenschutzgerechte Umsetzung. Im Bereich der Kraftfahrzeugindustrie muss damit bereits bei der Entwicklung von Systemen angesetzt werden. Es ist ein verantwortungsvoller Umgang mit den Daten zu fordern. Dies jedoch mit Blick auf die Erwartungen, die neben dem Markt auch das Recht und die Gesellschaft hinsichtlich des Datenschutzes und der Datensicherheit formulieren.

All die vorgenannten Aspekte spielen im Zusammenhang mit der Datenverwendung aus vernetzten Kraftfahrzeugen eine Rolle und sind bislang in rechtlicher Hinsicht nicht geklärt.

Kapitel 2: Das Kraftfahrzeug als "Datensammler"

Im Kraftfahrzeug fällt schon heute eine Vielzahl an Daten an, welche es einzeln und in Verknüpfung miteinander erlauben, eine Fülle an Informationen unter anderem über den Fahrer generieren und dadurch unter Umständen ein vollständiges Bewegungsprofil erzeugen zu können.

Teil 1: Die technischen Grundlagen

Um nachvollziehen zu können, welche Daten im Kraftfahrzeug generiert werden können, kommt es zunächst auf die technische Ausgestaltung an.[13] Dazu ist zunächst darzulegen, wie die Daten im Kraftfahrzeug in technischer Hinsicht verarbeitet werden.

I. Das Prinzip von Eingabe, Verarbeitung und Ausgabe

Bei dem sogenannten (sog.) *„EVA-Prinzip“* handelt es sich um ein Grundprinzip der Datenverarbeitung. Die Abkürzung ergibt sich aus der Reihenfolge, in der Daten verarbeitet werden, nämlich der *„Eingabe“* der Daten durch Sensoren[14], der *„Verarbeitung“* derselben im Steuergerät und der *„Ausgabe“* durch Aktoren.[15] Die durch die Sensoren ermittelten Kenngrößen, wie z. B. die Drehzahl werden mit den im Steuergerät vorhandenen Sollgrößen verglichen und für den Fall, dass diese nicht übereinstimmen, über die Aktoren mittels physikalischer Prozesse reguliert.[16]

---

13 Die technischen Grundlagen können im Rahmen dieser juristischen Arbeit nicht umfassend dargestellt werden. Es soll lediglich ein Überblick darüber gegeben werden, wie Daten im Kraftfahrzeug generiert werden.

14 *„Ein Sensor (von lateinisch sentire, dt. „fühlen“ oder „empfinden“), auch als Detektor, (Messgrößen- oder Mess-) Aufnehmer oder (Mess-) Fühler bezeichnet, ist ein technisches Bauteil, das bestimmte physikalische oder chemische Eigenschaften (z.B. Wärmestrahlung, Temperatur, Feuchtigkeit, Druck, Schall, Helligkeit oder Beschleunigung und/oder die stoffliche Beschaffenheit seiner Umgebung qualitativ oder als Messgröße quantitativ erfassen kann“*, vgl. http://de.wikipedia.org/wiki/Sensor.

15 Vgl. https://de.wikipedia.org/wiki/EVA-Prinzip.

16 Vgl. https://de.wikipedia.org/wiki/Steuergerät.

II. Die fünf Hauptanforderungen an Sensoren im Kraftfahrzeug

Sensoren im Kraftfahrzeug[17] müssen im Wesentlichen fünf Anforderungen genügen. Sie sind zunächst harten Betriebsbedingungen durch extreme Belastungen ausgesetzt. So müssen sie mechanische Angriffe in Form von Stößen und Vibrationen aushalten.[18] Auch Temperaturen in direkter Motornähe oberhalb von 120° C über mehrere Stunden müssen von den Sensoren bewältigt werden.[19] Sodann müssen Sensoren im Kraftfahrzeug eine hohe Zuverlässigkeit aufweisen. Diese orientiert sich absteigend an den Kategorien Passagierschutz, Motor und Komfort.[20] Aufgrund der steigenden Anzahl an Sensoren spielen auch die Aspekte niedriger Herstellungskosten und einer möglichst kleinen Bauweise eine große Rolle. Die Zielkosten von Sensoren in Kraftfahrzeugen werden mit 1,- bis 30,- Euro angesetzt.[21] Zuletzt kommt es auch auf eine hohe Genauigkeit der Sensoren an.[22] In Zukunft werden die Anforderungen an Sensoren durch den technischen Fortschritt aller Wahrscheinlichkeit nach noch ansteigen.

III. Die Arten von Sensoren im Kraftfahrzeug

Es gibt vielfache Möglichkeiten, Sensoren zu gruppieren. Für die Bearbeitung relevant wird hier die Differenzierung danach, ob es sich um Daten handelt, die durch das Kraftfahrzeug selbst oder aber durch Telematik- oder sog. Big Data-Anwendungen generiert werden und ob diese als fahrzeugbezogen oder fahrerbezogen zu bewerten sind. Dabei wird nochmals näher zu differenzieren sein, ob es sich dahingehend um datenschutzrelevante Daten handelt, weil diese Daten aufgrund ihrer Aussagekraft Konfliktpotenzial hinsichtlich der Befugnis des Umgangs mit den Daten aufweisen könnten. Bei der vorzunehmenden Einordnung soll es ebenfalls relevant sein, ob die Daten durch das Kraftfahrzeug bzw. im Kraftfahrzeug erzeugt werden oder ob dies durch den Einsatz von Fahrerassistenzsystemen oder beispielsweise Telematik-Anwendungen geschieht.

---

17 Die Darstellung beschränkt sich auf Sensoren im Kraftfahrzeug. Andere mögliche Anwendungsfelder für Sensoren werden nicht erörtert.

18 Vgl. *Reif*: Sensoren im Kraftfahrzeug, 2010, S. 25.

19 Vgl. *Reif*: Automobilelektronik, ^{4}2012, S. 99.

20 Unter die Kategorie „*Passagierschutz*“ fallen Lenkung und Bremse. Die Kategorie „*Motor*“ umfasst das Fahrwerk und die Reifen. Der „*Komfort*“ mit der niedrigsten Zuverlässigkeitsstufe meint ebenso Information wie Diebstahlsicherung. Vgl. *Reif*: Bosch Autoelektrik und Autoelektronik, ^{6}2011, S. 244.

21 Vgl. *Reif*: Sensoren im Kraftfahrzeug, 2010, S. 24

22 Vgl. *Reif*: Bosch Autoelektrik und Autoelektronik, ^{6}2011, S. 249

Teil 2: Datenerzeugung durch das Kraftfahrzeug selbst

Es ist heutzutage nicht mehr nur das Kraftfahrzeug selbst, welches Daten generiert. Durch die Verbindung von Telekommunikation mit dem Kraftfahrzeug gewinnen auch immer mehr sog. Telematik-Anwendungen an Bedeutung.[23] Die Speicherung der Daten im Kraftfahrzeug selbst erfolgt zunächst jeweils herstellerabhängig. Unterschieden wird grundsätzlich zwischen *„flüchtigen“*, *„semifesten“* oder *„festen“* Daten[24], wobei für die weitere Bearbeitung unterstellt werden muss, dass alle anfallenden Daten als feste Daten gespeichert werden. Dies ist bedingt dadurch, dass die Hersteller nahezu keine Informationen preisgeben, welche Daten von ihnen für welchen Zeitraum gespeichert werden und ob eventuell eine Übermittlung an externe Stellen stattfindet. Eingebaut werden Sensoren entweder bereits durch den Hersteller im Fertigungsprozess des Kraftfahrzeuges oder zu einem späteren Zeitpunkt durch Dritte (Arbeitgeber, Flottenbetreiber) z.B. in Gestalt einer Telematik-Box.[25]

I. Sensoren im Kraftfahrzeug - ein Überblick

Durch Sensoren werden im Kraftfahrzeug Daten generiert, die sich in fahrzeug- und fahrerbezogene Sensoren unterteilen lassen.[26] Obgleich es Sensoren bzw. Steuergeräte gibt, die offensichtlich Werte in Bezug auf den Fahrer liefern – wie z.B. den Müdigkeitswarner – so tun dies auch auf den ersten Blick unscheinbare Sensoren – wie z.B. die Wischwasseranzeige.[27] Deshalb soll an dieser Stelle ein Überblick gegeben werden, welche Daten von welchen Sensoren im Kraftfahrzeug generiert werden.[28]

1. Fahrzeugbezogene Sensoren

Als fahrzeugbezogene Sensoren werden an dieser Stelle diejenigen Sensoren eingeordnet, die ausschließlich bzw. weit überwiegend lediglich von technischer Bedeutung für

---

23 Vgl. dazu unter *Kapitel 2, Teil 4*.

24 Während flüchtige Daten direkt nach ihrer Erhebung genutzt und unmittelbar danach wieder gelöscht oder überschrieben werden, erfolgt bei semiflüchtigen Daten eine Speicherung für eine längere Zeitspanne, bevor die Daten gelöscht bzw. überschrieben werden. Die sog. festen Daten werden dauerhaft gespeichert; vgl. *Mielchen,* SVR 2014, S. 81-87 (82).

25 Vgl. *Kremer,* RDV 2014, S. 240-252 (241).

26 Für die später folgende rechtliche Beurteilung der Zulässigkeit des Umgangs mit den Daten kommt es maßgeblich darauf an, ob diese personenbezogen sind und bei wem die Daten relevant werden. Insoweit soll bereits hier eine Klassifizierung dahingehend erfolgen, ob und für wen die generierten Daten Relevanz besitzen. Die Einstufung bezüglich der Relevanz der Daten stellt die subjektive Betrachtungsweise der Bearbeiterin dar.

27 Vgl. *Eicher*, ADAC Motorwelt (4/2014), S. 16-20 (18).

28 Die Sensoren werden im Folgenden jeweils in alphabetischer Reihenfolge dargestellt.

das Kraftfahrzeug an sich sind und zunächst keine Informationen über die Person des Fahrers liefern. Fahrzeugbezogene Sensoren generieren entweder lediglich für eine kleine Interessengruppe relevante Daten oder solche, die für eine Vielzahl von Interesse sind und Konfliktpotenzial[29] dahingehend besitzen, wer in rechtlicher Hinsicht die Zugriffsbefugnis auf die Daten besitzt. Es kommt maßgeblich darauf an, für welche Interessengruppen die Daten letztlich relevant sind und welche Aussagekraft sie haben. Sofern lediglich ein technisches Interesse des Herstellers an den Daten besteht, kann zunächst davon ausgegangen werden, dass der Fahrer grundsätzlich vor solchen Daten nicht in datenschutzrechtlicher Hinsicht zu schützen ist.

a) Fahrzeugbezogene Sensoren von geringem Interesse

Einige fahrzeugbezogene Sensoren dienen weit überwiegend nur dem Betrieb und der technischen Überwachung des Kraftfahrzeugs. Insoweit werden die daraus generierten Daten zunächst nur für den Hersteller relevant. Für den Fahrer besitzen sie wegen der rein technischen Datensätze keine Relevanz. Diese Sensoren sind lediglich für Hersteller und Werkstätten zur Kundenansprache in Bezug auf Serviceleistungen und technischen Entwicklung wichtig.

Dazu zählt zunächst der ***Sensor für die Antriebsbatterie bei Elektrofahrzeugen***, der Informationen über das Batterieverhalten und die Nutzung gibt, weil dafür bislang kaum praktische Erfahrung vorhanden ist.[30]

Klopfsensor und Kraftstoffsensoren helfen, den Kraftstoffverbrauch zu reduzieren, indem sie den Motorlauf an Motorblockschwingungen und Kraftstoffqualität anpassen.[31]

Der ***Sensor für die Erkennung eines montierten Dachgepäckträgers*** passt das Anti-Schleuder-System an den durch den Dachgepäckträger resultierenden geänderten Fahrzeugschwerpunkt an.[32]

---

29 Konfliktpotenzial entsteht insbesondere dann, wenn eine Vielzahl von Akteuren wie beispielsweise Hersteller, Werkstätten, Versicherer, Flottenbetreiber und Fahrer gleichzeitig ein erhöhtes Interesse an den erzeugten Daten haben. Gerade solche Konfliktfälle werden hier eingestuft.

30 Deshalb werden die Daten bei den meisten Elektrofahrzeugen via Mobilfunk an den Hersteller übermittelt, um diese durch Analyse der Daten weiterentwickeln zu können.

31 Vgl. http://www.kienzle.de/index.php?104&backPID=104&tt_products=929.

Zuletzt besitzt der ***Sensor für die Position des Außenspiegels*** ebenfalls nur technische Relevanz.[33] Dieser ermittelt die Position des Außenspiegels. Anderweitige Erkenntnisse lassen sich aus den generierten Daten allein jedoch nicht gewinnen.

b) Fahrzeugbezogene Sensoren mit Konfliktpotenzial

Konfliktpotenzial können dahingegen Daten aufweisen, die zwar ebenfalls lediglich fahrzeugbezogen sind, aber im Ergebnis für verschiedenste Interessengruppen relevant und vor allem für den Fahrer im Verhältnis zu Herstellern, Werkstätten, Versicherungen und Flottenbetreibern von Bedeutung sein können. Hierbei gibt es Sensoren, die im Hinblick auf Garantie[34]- und Kulanzansprüche des Halters wegen Wartungsmängeln relevant werden und solche, die eventuell Rückschlüsse auf das Fahrverhalten des Fahrers zulassen und deshalb für den Fahrer gegenüber Dritten datenschutzrechtliche Relevanz haben. Auch hier spielt die Kundenansprache durch Werkstätten eine Rolle, soweit hier eine Ansprache in Bezug auf das Fahrverhalten vorliegt.

Zunächst können die aus Sensoren generierten Daten Hinweise auf mangelnde Wartung geben mit der Folge, dass aufgrund dessen durch Hersteller oder Werkstätten Garantie- und Kulanzansprüche oder durch Versicherungen die Übernahme von Versicherungsfällen abgelehnt werden könnten.

Der ***Batteriespannungs-Sensor*** dient insbesondere bei Fahrzeugen mit Start-Stopp-Automatik dem Betrieb und der Überwachung des Ladezustands.[35] Dem Hersteller wird dadurch die Kundenansprache bei einem notwendigen Batterietausch möglich. Allerdings wird dadurch auch eine etwaige mangelnde Wartung durch den Halter erkennbar.

Ähnlich verhält es sich mit dem ***Bremsdrucksensor***, der den Bremsdruck des durch den Fahrer betätigten Bremspedals erfasst und die Information an das Bremssystem weiterleitet. Die dabei erzeugten Daten, wie z.B. das Datum, dass zu hart gebremst wurde, können ebenfalls im Rahmen von Garantie- und Kulanzansprüchen relevant werden.

---

32 Vgl. http://www.adac.de/_ext/itr/tests/Autotest/AT4158_Audi_Q5_20_TDI_quattro/Audi_Q5_20_TDI_quattro.pdf.

33 Anders beurteilt sich dies für den Sensor zur Position der Vordersitze und der Kopfstütze, vgl. dazu unter *Kapitel 2, Teil 2, I.2.b)*.

34 Im Jahr 2010 ist der Autohersteller Nissan dazu übergegangen, Ansprüche aus einer Garantie abzulehnen, wenn der Kunde den Zugriff auf die „*Black Box Data*“ verweigert, vgl. http://jalopnik.com/5201918/2010-gt-r-warranty-voided-for-denying-nissan-access-to-your-black-box-data/all.

35 Vgl. *Braess/Seiffert*: Vieweg Handbuch Kraftfahrzeugtechnik, [7]2013, S. 456.

Der ***Bremsflüssigkeitsstandsensor*** löst – wie sich bereits aus dem Wortlaut ergibt – eine Warnung aus, wenn zu wenig Bremsflüssigkeit vorhanden ist. Relevant für Gewährleistungsansprüche kann hier die Erkenntnis sein, dass die Bremsflüssigkeit trotz Warnung nicht rechtzeitig vom Halter bzw. Fahrer nachgefüllt wurde.

Der ***Gaspedalsensor*** vermittelt, wie schnell und wie weit das Gaspedal getreten wurde. Als Fahrpedalsensor erfasst er den Weg und die Winkelposition des Pedals.[36]

Die ***Getriebesensoren***[37] und die ***Motorsensoren***[38] sind für die Getriebe- bzw. Motorfunktion erforderlich. Durch sie ist jeweils ein Rückschluss darauf möglich, ob der Fahrer umsichtig fährt oder aber ein unsachgemäßer Umgang mit dem Triebwerk durch Fahren mit überhöhter Drehzahl vorliegt.

Der ***Kühlmittelstandssensor*** löst bei Mängeln eine Warnanzeige aus.

Durch den ***Reifendrucksensor*** und den ***Sensor für den Waschwasserstand***, die den Reifendruck bzw. den Füllstand des Waschwasserbehälters überwachen, werden im Notfall Warnmeldungen im Cockpit aktiviert. Eine längere Aktivierung kann dabei ein Anzeichen für schlechte Wartung durch den Halter oder Fahrer sein. Dies kann je nach vertraglicher Ausgestaltung dazu führen, dass seitens des Herstellers oder der Werkstätten Garantie- und Kulanzansprüche abgelehnt werden könnten.

Andere Sensoren erzeugen Daten, die Rückschlüsse auf das Fahrverhalten oder eine Fehlbedienung seitens des Fahrers zulassen.

Der ***Alarmanlagensensor*** ist dazu ausgelegt, unberechtigte Zugangsversuche und Bewegungen im Innenraum akustisch anzuzeigen.[39] Vor allem interessiert an solchen Daten sind Flottenbetreiber, Versicherungen, aber auch öffentliche Behörden zur Aufklärung von Diebstählen und zum Auffinden des Kraftfahrzeugs. Die Daten lassen jedoch auch Rückschlüsse darauf zu, ob der Fahrer eventuell seine Sorgfaltsplicht verletzt haben könnte.

---

36 Vgl. *Reif*: Sensoren im Kraftfahrzeug, 2010, S. 138.

37 Dies sind bei Direktschaltgetriebe/Automatik für eingelegten Gang insbesondere Ein- und Ausgangsdrehzahl, Kupplungstemperatur, Steuergerätetemperatur und Öltemperatur.

38 Darunter fallen insbesondere Kurbel- und Nockenwellendrehzahl und –stellung, Unterdruck, Luftmasse, Ansaugluft-Temperatur, Luftdruck, Öl-Temperatur/-qualität/-stand, Sauerstoff-Speichervermögen des Katalysators und Ruß-Beladung des Partikelfilters.

39 Vgl. https://de.wikipedia.org/wiki/Kfz-Alarmanlage.

Durch den ***Anhängerkupplungssensor*** kann kontrolliert werden, ob eine klappbare Anhängerkupplung korrekt verriegelt wurde.[40] Durch eine aufleuchtende Signallampe im Cockpit kann eine Fehlbedienung seitens des Fahrers erkannt werden.

Der ***Bremsbelagverschleiß-Sensor*** warnt im Cockpit davor, dass verschlissene Bremsbeläge ausgetauscht werden müssen.[41] Die Daten können beim Hersteller dazu genutzt werden, durchschnittliche Wechselintervalle anhand der Fahrweise zu berechnen und Kunden anzusprechen.

Auch wird durch ***Fahrwerksbereichssensoren*** die Karosseriebeschleunigung festgestellt.[42] Die Tatsache, dass ein Kraftfahrzeug oft überladen oder auf unbefestigten Wegen gefahren wird, könnte dem Fahrer von Versicherungen und Werkstätten entgegen gehalten werden.

Der für das Anti-Schleuder-System notwendige ***Kupplungspedalsensor*** gibt Auskunft darüber, in welcher Stellung sich das Kupplungspedal befindet. Er erfasst den Weg bzw. die Winkelposition des Kupplungspedals.[43] Eine Fehlbedienung durch Schleifenlassen könnte dadurch seitens des Herstellers nachgewiesen werden.

Zuletzt kann durch den ***Sensor für offene Türen oder Klappen*** im Cockpit ein Alarmsignal ausgelöst werden. Dadurch wird beispielsweise der Nachweis möglich, dass unzulässigerweise mit offener Heckklappe gefahren und diese dabei beschädigt wurde.

Sämtliche vorgenannten Sensoren haben Aussagekraft für Dritte und sind somit aus verschiedenen Gründen für unterschiedliche Gruppen von Interesse. Da jeweils Rückschlüsse auf ein etwaiges Fehlverhalten des Fahrers bzw. Halters möglich sind, muss davon ausgegangen werden, dass eine datenschutzrechtliche Relevanz gegeben ist.

2. Fahrerbezogene Sensoren

Es gibt aber auch Sensoren, die sich nicht nur auf den Betrieb des Kraftfahrzeugs beziehen, sondern insbesondere auf den Fahrer an sich bezogene Daten generieren.

---

40 Vgl. http://www.rockinger-agriculture-catalogue.com/de/zubehoer/sicherheitssensor.html?country=1&L=0&header=lof.

41 Vgl. https://de.wikipedia.org/wiki/Bremsbelag.

42 Vgl. *Reif*: Sensoren im Kraftfahrzeug, 2010, S. 75.

43 Vgl. *Reif*: Sensoren im Kraftfahrzeug, 2010, S. 138.

a) Fahrerbezogene Sensoren von geringem Interesse

Manche dienen lediglich dazu, dem Fahrer die Bedienung des Kraftfahrzeugs zu erleichtern und fungieren als reine Komfortsensoren.

Der ***Sensor für automatisch abblendbare Spiegel*** erkennt beispielsweise einen mit Fernlicht fahrenden Hintermann und blendet die Innen- und Außenspiegel daraufhin automatisch ab.[44] Dies dient ausschließlich dazu, dem Fahrer die Fahrt zu erleichtern, damit dieser in diesem Fall nicht mehr händisch den Spiegel verstellen muss. Lediglich der Hersteller und die Werkstatt sind für Verbesserungen der Funktion an solchen Daten interessiert.

Der ***Klimaanlagensensor***[45] erzielt das Klima, das den Wünschen des Fahrers entspricht.

In immer mehr Kraftfahrzeugen sind auch sog. ***Luftgütesensoren*** eingearbeitet. Sobald ein bestimmter Schwellenwert an Schadstoffen im Fahrzeug erreicht ist, wird automatisch die Umluftschaltung aktiviert.[46] Dadurch muss der Fahrer nicht mehr ständig die Lüftung selbst bedienen. Vielmehr übernimmt das Kraftfahrzeug die Einstellung durch den Luftgüte-Sensor selbst.[47] Zudem wird ein erhöhter Kohlendioxidgehalt verhindert, der zu Müdigkeit, Unwohlsein und körperlichen Beschwerden führen kann.[48]

Zuletzt sei im Bereich des Komforts für den Fahrer der ***Regen-Licht-Sensor*** genannt. Er erkennt feinste Tropfen auf der Scheibe und aktiviert die automatische Betätigung des Scheibenwischers.[49] Diese reinen Komfortsensoren generieren insgesamt keine relevanten Daten.

b) Fahrerbezogene Sensoren mit Konfliktpotenzial

Die aus den folgenden Sensoren generierten Daten betreffen jedoch wiederum die Interessen unterschiedlichster Gruppen, sodass insoweit Konfliktpotential bezüglich einer etwaigen Zugriffsbefugnis besteht und dadurch diese Daten im datenschutzrechtlichen

---

44 Vgl. http://www.volkswagen.de/de/technologie/technik-lexikon/innenspiegel_automatischabblendend.html.

45 Dieser erfasst Außen- und Innentemperatur, Intensität und Richtung der Sonneneinstrahlung, Kältemitteldruck, Ausströmtemperaturen im Innenraum, Beschlagneigung der Frontscheibe, Fahrervorwahl und Verdampfertemperatur.

46 Vgl. https://de.wikipedia.org/wiki/Luftgütesensor.

47 Vgl. http://www.road-and-motor.ch/de/wissen/auto-moto-technologie/detail/sensoren-unserem-auto.

48 Vgl. *Reif*: Sensoren im Kraftfahrzeug, 2010, S. 166.

49 Vgl. *Reif*: Sensoren im Kraftfahrzeug, 2010, S. 158.

Sinne als relevant einzustufen sind. Viele der Daten sind insbesondere für Unfallgeschehen und dessen Abwicklung zwischen den verschiedenen Interessengruppen relevant.

Der ***Augenlidersensor*** beispielsweise warnt den Fahrer vor dem Sekundenschlaf.[50] Er gibt also einen Hinweis auf eine etwaige Ablenkung des Fahrers. Hersteller und Werkstatt, Versicherungen, aber auch Flottenbetreiber haben ein großes Interesse daran zu wissen, ob ein Unfall unter Umständen auf Sekundenschlaf des Fahrers zurückzuführen ist.

Ähnlich verhält es sich mit dem ***Blinkerhebel-Sensor***. Es wird dabei erfasst, wann die Blinkerleuchten angesteuert wurden.[51] Auf den ersten Blick erscheint dieser Sensor unverfänglich. Doch kann dieser insbesondere für die Rekonstruktion eines Unfallhergangs relevant werden.

Der ***Crashsensor***[52] erkennt bei einem Unfall einen Aufprall oder Überschlag und sendet diese Informationen an Insassenschutzsysteme, wie z.B. den Airbag.[53]

Für den Fahrer gegenüber Werkstätten, Herstellern, Versicherungen, Behörden und Flottenbetreibern von hoher Relevanz ist auch der ***Sensor für das Global Positioning System (GPS).*** Damit ist die Ermittlung der Position des Kraftfahrzeugs auf Satellitenbasis[54] möglich.[55] GPS ermöglicht sozusagen eine lückenlose Aufzeichnung von Bewegungsdaten.[56] Für die aus dem GPS-Sensor erzeugten Daten ist eine vielfältige Verwendung denkbar. Der sich aus dem Raddrehzahl-Sensor ergebende Drehzahlwert kann zur Berechnung zurückgelegter Strecken dienen.[57] Im Ergebnis ist der GPS-Sensor also nicht nur für den Fahrer von hoher Relevanz. Auch für Hersteller, Werkstätten, Versicherungen und Behörden besteht ein großes Interesse an diesen Daten. Die hier erzeugten Daten sind zudem relevant für weitere Insassen.

---

50 Der Augenlider-Sensor ist Teil des Aufmerksamkeits-Assistenten, der im Rahmen der Fahrerassistenzsysteme näher dargestellt wird, vgl. unter *Kapitel 2, Teil 3, II.2.*.

51 Verknüpft mit anderen Daten können allerdings auch im Hinblick auf die z.B. durch den Blinkerhebel generierten Daten Konflikte entstehen, vgl. unter *Kapitel 2, Teil 5, I.*.

52 Dieser wird auch Aufprallsensor genannt.

53 Vgl. https://de.wikipedia.org/wiki/Crashsensor.

54 Für GPS sind mittlerweile 31 Satelliten verfügbar, vgl. http://www.navcen.uscg.gov/?Do=constellationStatus.

55 Vgl. *Reif*: Sensoren im Kraftfahrzeug, 2010, S. 65.

56 Vgl. *Biegel*: Überwachung von Arbeitnehmern durch technische Einrichtungen, 2000, S. 7.

57 Vgl. http://www.mein-autolexikon.de/elektronik/sensoren.html.

Auch der ***Gurtschlosssensor*** sowie der ***Sitzbelegungssensor*** sind nicht nur für den Fahrer, sondern auch für Dritte als Insassen von Relevanz. Diese Sensoren erkennen, ob ein Sitz belegt ist und der dazugehörige Gurt im Gurtschloss steckt. Es kann ermittelt werden, wer angeschnallt war. Durch die Sitzbelegungserkennung und den Gurtschloss-Sensor weiß das Fahrzeug, welcher Sitz belegt ist und löst eine Anschnall-Erinnerung aus, falls ein Insasse nicht angeschnallt ist.[58]

Der ***Längs- und Querbeschleunigungssensor*** wird im Rahmen des Elektronischen Stabilitätsprogramms (ESP)[59] genutzt. Die dort erzeugten Daten geben Aufschluss über die Fahrweise des Fahrers, was unter Umständen auch zur Ablehnung von Garantie- oder Kulanzansprüchen gegen Hersteller oder Werkstätten führen kann.

Auch die ***Lenksensoren***[60] werden für das ESP genutzt.[61] Zusätzlich ist es möglich, über diese eine Pausenempfehlung an den Fahrer zu senden.[62]

Neu sind ***medizinische Sensoren*** im Kraftfahrzeug. Zukünftig erfasst das Kraftfahrzeug Atemalkoholgehalt[63], Herzfunktion[64] sowie psychische Verfassung des Fahrers und kann bei Auffälligkeiten z.B. die Warnblinkanlage automatisch einschalten[65] oder das Kraftfahrzeug autonom zum Stehen bringen.[66] Wissenschaftler haben eine lenkradintegrierte Sensoreinheit entwickelt, die Vitalparameter wie z.B. die Herzfrequenz über Sensoren im Lenkrad ermittelt.[67] Insgesamt greift dies natürlich sehr weit in den persönlichen Bereich des Fahrers ein. Eine Relevanz der Daten lässt sich nicht leugnen. Sie betreffen hinsichtlich seines Gesundheitszustandes seine Intimsphäre.[68]

Der ***Sensor für die Position der Vordersitze und der Kopfstützen*** dient der elektrischen Verstellung derselben und wird für die Memory-Funktion genutzt, mit der die individuelle Sitzeinstellung des Fahrers gespeichert und per Knopfdruck wiederhergestellt wer-

---

58 Vgl. https://de.wikipedia.org/wiki/Gurtschloss.
59 Vgl. unter *Kapitel 2, Teil 3*.
60 Darunter fallen der Lenkradbewegungs- und Lenkmomentsensor sowie der Lenkwinkelsensor.
61 Vgl. *Reif*: Sensoren im Kraftfahrzeug, 2010, S. 140.
62 Vgl. http://www.elektroniknet.de/automotive/sonstiges/artikel/87362/.
63 Sog. Alcolock-System, vgl. http://www.shortnews.de/id/884387/volvo-verbaut-alcolocks.
64 Vgl. http://www.presseportal.de/print/2544042-s-max-concept-zeigt-die-moeglichkeiten-von-deisgn-und-technologie-kommender.html.
65 Vgl. http://www.experto.de/b2c/gesundheit/krankheiten/herz/wenn-das-auto-auf-das-herz-aufpasst.html.
66 Vgl. https://de.wikipedia.org/wiki/Fahrerassistenzsystem.
67 Vgl. http://www.medizin-und-technik.de/autos/-/article/27544623/35127697/Auto-fahren,-statt-den-Arzt-zu-besuchen/art_co_INSTANCE_0000/maximized/.
68 Vgl. https://de.wikipedia.org/wiki/Intimsphäre.

den kann.[69] Dies kann Hinweise darauf geben, dass Lehne oder Gurthöhe falsch bzw. zu schräg eingestellt gewesen sind und es deshalb z.B. zu unnötig hohen Verletzungen bei einem Unfall gekommen ist.

Der ***Unfalldatenspeicher (UDS)***[70] wird auf freiwilliger Basis eingebaut und zeichnet Daten[71] des Fahrzeugs im Falle eines Unfalls mindestens für die letzten 30 Sekunden auf, bevor sie automatisch gelöscht werden.[72] Dem Fahrer dürfte in diesem Fall ausnahmsweise bekannt sein, dass und vor allem welche Daten gespeichert werden. Insofern kann sich der freiwillige Einbau auch auf die Fahrweise auswirken. Jedenfalls werden die Unfalldaten für sämtliche Interessengruppen relevant, sei es für Versicherungen, Behörden oder Flottenbetreiber. Ebenso ist eine hohe Relevanz bezüglich der Daten für den Fahrer gegeben.

Zuletzt sei das ***Videokamerasystem***[73] eines Kraftfahrzeugs aufgeführt. Nach vorn gerichtet[74] ist durch die Kamera die Erkennung von Verkehrsschildern und Fahrbahnmarkierungen möglich. Nach vorn, zur Seite und nach hinten gerichtet kann dadurch die Umgebung des Kraftfahrzeugs dargestellt werden. Auf den Fahrer gerichtet gibt die Kamera Aufschluss darüber, ob der Fahrer möglicherweise abgelenkt oder unkonzentriert ist, aber auch, ob er gesundheitliche Probleme aufweist. Zumindest in diesem Fall ist ohne Umschweife die Relevanz der Daten für den Fahrer gegeben.

---

69 Vgl. http://www.bmw.de/de/footer/publications-links/technology-guide/sitzverstellung-elektrisch-memory.html.

70 Die internationale Bezeichnung lautet „*Event Data Recorder*“ (EDR).

71 Aufgezeichnet werden z.B. Geschwindigkeit, Bewegungsrichtung, Blinkerbestätigung und Bremstätigkeit.

72 Vgl. https://de.wikipedia.org/wiki/Unfalldatenspeicher.

73 Ob es sich bei den einzelnen Kameras um Mono- oder Stereokameras handelt, ist nicht entscheidungserheblich, vgl. dazu *Schöttle*: Meilensteine auf dem Weg zum autonomen Fahren, http://www.springerprofessional.de/meilensteine-auf-dem-weg-zum-autonomen-fahren/5155132.html.

74 Die Problematik der Zulässigkeit sog. Dashboard-Cams soll hier nicht weiter vertieft werden; vgl. insoweit Amtsgericht München, Urteil vom 06.06.2013, Aktenzeichen 343 C 4445/13, in: NJW-RR 2014, S. 413-415 sowie Verwaltungsgericht Arnsbach, Urteil vom 12.08.2014, Aktenzeichen AN 4 K 13.01634, in: DAR 2014, S. 663-667. Während das AG München über die Zulässigkeit der Videoaufnahmen aus Dashcams als Beweismittel im Zivilprozess zu entscheiden hatte und nach Abwägung der gegenseitigen Interessen zum dem Ergebnis kam, die Verwendung sei zulässig, musste das VG Arnsbach einer Klage eines Rechtsanwalts als Fahrer eines Fahrzeuges mit eingebauter Dashcam allein wegen eines Formmangels stattgeben, obwohl das Gericht bei der Abwägung der widerstreitenden Interessen nach dem Bundesdatenschutzgesetz der Auffassung war, die Interessen des Klägers müssten hinter denen der betroffenen Öffentlichkeit zurücktreten.

3. Zusammenfassung

Dieser Abschnitt hat gezeigt, welche Daten in einem Kraftfahrzeug durch verschiedenste Sensoren generiert werden können und welche Auswirkungen dies für den Fahrer bedeuten kann. Dies sei als Grundlage für die sich anschließende rechtliche Würdigung zu sehen.

II. Die Vernetzung im Kraftfahrzeug

Viele der Daten aus den vorgenannten Sensoren werden in unterschiedlichen Steuergeräten benötigt. Um die Rechenleistung jeweils nur einmal erbringen zu müssen, ist es sinnvoll, die Daten in einem Steuergerät zu verarbeiten und an andere Steuergeräte weiterzuleiten.[75] Im modernen Fahrzeug kommunizieren Sensoren, Steuergeräte und Aktoren untereinander über sog. Bussysteme.[76] Es ist zu unterscheiden zwischen dem sog. CAN-Bus[77] für die Bereiche Antrieb, Fahrwerk und Karosserie sowie dem sog. MOST-Bus[78] für Multimedia.[79] Als kostengünstige Alternative zur Vernetzung von intelligenten Sensoren und Aktoren wurde der sog. LIN-Bus entwickelt.[80] Die Bussysteme erhöhen die Kommunikationsfähigkeit der Systeme im Kraftfahrzeug.[81] Dadurch wird die optimale Vernetzung sämtlicher Sensoren im Kraftfahrzeug realisiert.

III. Verarbeitung der Daten im Steuergerät

Die über das Bussystem an die Steuergeräte weitergeleiteten Daten werden dort verarbeitet. Dies soll hier am Beispiel des Airbag-Steuergerätes dargestellt werden.

---

75 Beispielsweise wird die Fahrgeschwindigkeit im ESP für die Fahrdynamikregelung, im Autoradio für die geschwindigkeitsabhängige Lautstärkenregelung und im Tempomat für die automatische Geschwindigkeitsregelung genutzt, vgl. *Reif*: Bosch Autoelektrik und Autoelektronik, ^{6}2011, S. 82.

76 Die Abkürzung „*BUS*“ steht für „*Binary Unit System*“. Das Bussystem wird häufig verglichen mit einem Omnibus, bei dem dieser die gesamte Fahrstrecke abfährt und die Fahrgäste selbständig an den für sie passenden Haltestellen aussteigen, vgl. dazu http://de.wikipedia.org/w/index.php?oldid=130390638.

77 Die Abkürzung „*CAN*“ steht für „*Control Area Network*“, vgl. https://de.wikipedia.org/wiki/Controller_Area_Network.

78 Die Abkürzung “*MOST*” steht für „*Media Oriented Systems Transport*“, vgl. https://de.wikipedia.org/wiki/MOST-Bus.

79 Vgl. *Wallentowitz*: Handbuch Kraftfahrzeugelektronik, ^{1}2006, S. 180.

80 Die Abkürzung “*LIN*” steht für „*Local Interconnect Network*“, vgl. https://de.wikipedia.org/wiki/Local_Interconnect_Network.

81 Eine weitergehende Vertiefung der technischen Ausgestaltung der Vernetzung in Fahrzeugen wird nicht vorgenommen. Für die rechtliche Betrachtung ausschlaggebend ist allein die Feststellung, dass die Systeme untereinander und miteinander vernetzt sind. Dadurch wird deutlich, dass ein und dieselbe Information an verschiedenen Stellen im Kraftfahrzeug vorhanden sein kann.

1. Das Steuergerät im Kraftfahrzeug

Die Signale aus den Sensoren werden über die Bussysteme dem Steuergerät als Schaltzentrale der Motorsteuerung zugeführt und dort aufbereitet und die Ausgangssignale zur Ansteuerung der Aktoren berechnet.[82] Grundsätzlich überwachen dabei alle gängigen Steuergeräte ihren Betrieb selbständig im Wege der elektronischen Fahrzeugdiagnose, der sog. On-Board-Diagnose (OBD).[83] Gesetzlich vorgeschrieben ist dies jedoch nur für die Fahrzeugdiagnose zur Überwachung der Wirkungsweise emissionsrelevanter Teile im Kraftfahrzeug.[84] Die Ermächtigungsgrundlage für die Verwendung dieser anfallenden Daten ist enthalten in Art. 5 Abs. 3 der Verordnung (EG) 715/2007[85].

2. Die Datenverarbeitung am Beispiel des Airbag-Steuergeräts

Die Volkswagen Aktiengesellschaft beschreibt die Vorgänge im Steuergerät wie folgt:

> *„Das Airbag-Steuergerät erkennt und bewertet einen Crash und aktiviert entsprechend der Unfallart und -schwere die jeweiligen Rückhaltesysteme. Seine Informationen erhält das Steuergerät über bis zu sechs externe Beschleunigungssensoren (Crash-Sensoren). (...) Die Sensoren im Steuergerät dienen dazu, die Signale der anderen Sensoren zu bewerten und abzugleichen. Dies ermöglicht dem Steuergerät, die Richtung des Unfalls und die Schwere einzuschätzen und für die Auslösung der entsprechenden Rückhaltesysteme zu sorgen. Über die Crash-Signalausgänge ist das Steuergerät mit weiteren CAN-Datenbussystemen verbunden, um nach einem Unfall Orientierung und Bergung der Insassen zu erleichtern."*[86]

Dies belegt, dass eine Vielzahl an Sensoren mit dem Steuergerät verbunden ist und deren Informationen dort zusammengefasst und aufbereitet werden. Nur durch diese Vernetzung ist eine optimale Nutzung aller vorhandenen Daten möglich.

---

82 Vgl. *Reif*: Bosch Autoelektrik und Autoelektronik, [6]2011, S. 198 f..

83 Vgl. http://de.wikipedia.org/w/index.php?oldid=132962136.

84 Die Funktionsfähigkeit wird im Rahmen der allgemeinen Straßenverkehrszulassung durch Behörden und auch im Rahmen der regelmäßig durchzuführenden Abgasuntersuchung (AU) geprüft, vgl. https://de.wikipedia.org/wiki/Fahrzeugdiagnose.

85 *Verordnung (EG) Nr. 715/2007 des Europäischen Parlaments und des Rates vom 20. Juni 2007 über die Typgenehmigung von Kraftfahrzeugen hinsichtlich der Emissionen von leichten Personenkraftwagen und Nutzfahrzeugen (Euro 5 und Euro 6) und über den Zugang zu Reparatur- und Wartungsinformationen für Fahrzeuge vom 29.06.2007*, ABl. Nr. L 171 S. 1. Die OBD soll jedoch im Rahmen der Untersuchung nicht weiter vertieft werden.

86 Vgl. http://www.volkswagen.de/de/technologie/technik-lexikon/airbag-steuergeraet.html.

IV. Die Ausgabe der Daten durch Aktoren

Die Ausgabe der Daten durch die Aktoren stellt den letzten Schritt im Rahmen des sog. EVA-Prinzips[87] dar. Aktoren setzen die von den Steuergeräten ausgehenden elektrischen Signale in einen mechanischen Prozess oder andere physikalische Größen, wie z.B. Druck um und greifen dadurch aktiv in das Regelungssystem des Kraftfahrzeugs ein.[88] Damit bilden sie die Schnittstelle zwischen der Datenverarbeitung in den einzelnen Steuergeräten und dem darauffolgenden mechanischen Prozess zur Umsetzung der Signale und Ausgabe der Daten.[89]

Teil 3: Fahrerassistenzsysteme

Neben den Sensoren, die Daten aus dem Kraftfahrzeug selbst erzeugen, gibt es eine Reihe sog. Fahrerassistenzsystemen. Diese zeichnen sich durch die Besonderheit aus, dass sie teilautonom oder autonom in Antrieb und Steuerung des Kraftfahrzeugs eingreifen oder alternativ den Fahrer durch eine geeignete Mensch-Maschine-Schnittstelle vor kritischen Situationen warnen.[90] Es handelt sich mithin um den Fahrer unterstützende und ihm assistierende Systeme.[91]

I. Rechtliche Grundlagen und Funktionsweise von Fahrerassistenzsystemen

Die Aufgabe von Fahrerassistenzsystemen ist es, den Fahrer bei seiner primären Fahraufgabe zu unterstützen, ihn zu informieren und zu warnen, sowie Komfort und Sicherheit durch aktive Fahrzeugführung und Fahrzeugstabilisierung zu erhöhen.[92] Die Assistenzfunktion reicht von Information über Unterstützung bis hin zur Übernahme von Fahrhandlungen.[93] Fahrerassistenzsysteme sind zurzeit so ausgestaltet, dass der Fahrer diese jederzeit übersteuern kann, die Verantwortung über das Kraftfahrzeug behält und er nicht durch die Fahrerassistenzsysteme sozusagen entmündigt werden kann.[94] Dies folgt aus den gesetzlichen Regelungen des *„Wiener Übereinkommens vom 08. Novem-*

---

87 Vgl. unter *Kapitel 2, Teil 1, I.*.
88 Vgl. https://de.wikipedia.org/wiki/Aktor.
89 Vgl. *Reif*: Bosch Autoelektrik und Autoelektronik, ^{6}2011, S. 376.
90 Vgl. https://de.wikipedia.org/wiki/Fahrerassistenzsystem.
91 Die Darstellung beschränkt sich auf die geläufigsten Fahrerassistenzsysteme und ist aufgrund der Fülle an Fahrerassistenzsystemen und ständig neuer Entwicklungen in diesem Bereich nicht als abschließend zu verstehen.
92 Vgl. *Reif*: Fahrstabilisierungssysteme und Fahrerassistenzsysteme, 2010, S. 104.
93 Vgl. *Deutschle*, SVR 2005, S. 249-254 (253).
94 Vgl. https://de.wikipedia.org/wiki/Fahrerassistenzsystem.

ber 1968 über den Straßenverkehr" (WÜ-StV).[95] Eine Sonderstellung nehmen lediglich Fahrdynamikregelsysteme wie z.B. das ESP ein, bei denen eine Übersteuerbarkeit während des Eingreifens nicht mehr möglich ist. Allerdings setzen sie den Fahrerwunsch in einer zeitkritischen Situation so gut wie möglich um und sind deshalb im Ergebnis dennoch als zulässig zu erachten.[96]

Die wachsende Flut an Informationen, die der Fahrer zu verarbeiten hat, muss ihm über geeignete Anzeigemedien und in ergonomisch sinnvoller Art und Weise übermittelt werden.[97] Dies geschieht über sog. Mensch-Maschine-Schnittstellen.[98] Diese befinden sich im Kraftfahrzeug an unterschiedlichen Stellen und in unterschiedlichen Formen. Bei der Mittelkonsole handelt es sich exemplarisch ebenso um eine solche Schnittstelle, wie auch bei der Windschutzscheibe. Letztere soll zukünftig durch das sog. Head-Up-Display (HUD) ergänzt werden. Dabei werden ausgewählte fahrrelevante Informationen von einem vollfarbigen TFT[99]-Display auf die Windschutzscheibe projiziert, sodass der Eindruck entsteht, es gebe in zwei bis drei Metern Entfernung eine frei schwebende Anzeige.[100] Üblich ist jedoch bislang die Anzeige- und Bedieneinheit in der Mittelkonsole. Dazu gehören u.a. das Autoradio, sämtliche Bedienelemente für Funktionen des Kraftfahrzeugs, Anzeigen für Geschwindigkeit und Navigationssystem, aber auch die Integration des Mobiltelefons. Soweit vorgesehen ist, dass das Fahrerassistenzsystem den Fahrer vor einer gefährlichen Situation warnt, geschieht dies durch optische, akustische, sprachliche oder haptische[101] Zeichen.[102] Sofern einige Fahrerassistenzsysteme[103] neben den Informationen über die Fahrsituation zusätzliche Informationen über das Fahrzeugumfeld benötigen, basiert diese Umfelderfassung alternativ bzw. kumulativ auf Ultraschall, Radar, Lidar und Kamera.[104] Obwohl einige Fahrerassistenzsysteme für ihre Anwendung meist lediglich nur einen Sensor brauchen, geht der Trend hin zur sog. Sensordatenfusion. Die Fusion beispielsweise von Fahrdynamikdaten und Signalen des

---

95 *Wiener Übereinkommen über den Straßenverkehr vom 08. November 1968 (mit Anhängen)*, http://www.admin.ch/opc/de/classified-compilation/19680244/index.html sowie unter *Kapitel 2, Teil 6*: Ausblick: Autonomes Fahren in der Zukunft.

96 Vgl. *Reif*: Bosch Autoelektrik und Autoelektronik, ^{6}2011, S. 323.

97 Vgl. *Reif*: Fahrstabilisierungssysteme und Fahrerassistenzsysteme, 2010, S. 122.

98 Andere Bezeichnungen dafür sind z.B. auch „*Human Machine Interface*" (HMI) oder „*Man Machine Interface*" (MMI).

99 Die Abkürzung „*TFT*" steht für „*Thin-film transistor*".

100 Vgl. *Siebenpfeiffer*: Vernetztes Automobil, 2014, S. 138.

101 Haptisch meint den Tastsinn betreffend, vgl. http://www.duden.de/suchen/dudenonline/haptisch.

102 Vgl. *Reif*: Fahrstabilisierungssysteme und Fahrerassistenzsysteme, 2010, S. 127.

103 Genannt sei an dieser Stelle beispielhaft nur der Abstandsregeltempomat, der im Nachgang noch genauer dargestellt wird, vgl. unter *Kapitel 2, Teil 3, II.3.*.

104 Vgl. https://de.wikipedia.org/wiki/Fahrerassistenzsystem.

GPS ermöglicht im Ergebnis eine spurgenaue Positionsbestimmung.[105] Die zukünftigen Möglichkeiten durch Fusion von verschiedenen Sensordaten erscheinen grenzenlos.

II. Datenerzeugung durch Fahrerassistenzsysteme

Fahrerassistenzsysteme lassen sich anhand verschiedener Fahrhandlungen differenzieren und eingruppieren. Auch hierbei soll bereits eine Bewertung einfließen, ob die erzeugten Daten in datenschutzrechtlicher Hinsicht Relevanz besitzen.

1. Fahren und Parken

Zunächst gibt es Fahrerassistenzsysteme, die den Fahrer beim Fahren selbst und beim Parken unterstützen.

Antiblockiersystem (ABS)[106]**,** ***Antriebsschlupfregelung (ASR)***[107] und ***ESP***[108] dienen vorwiegend der Sicherheit des Fahrers im Straßenverkehr. Die dazu notwendigen Daten werden durch Ermittlung der Raddrehzahl gewonnen. Das jeweilige Drehzahlsignal wird mittels Kabel an die Steuergeräte von ABS, ASR oder ESP weitergeleitet, die die Bremskraft je Rad individuell regeln.[109] Allerdings lässt sich dadurch auch die zurückgelegte Fahrstrecke feststellen bzw. ob eher kurze oder lange Strecken gefahren werden. Dies wiederum könnte dem Fahrer entgegengehalten werden, sodass davon auszugehen ist, dass der Fahrer vor diesen Daten zu schützen sein wird.

Der ***Aufmerksamkeitsassistent*** soll Unfälle durch Sekundenschlaf des Fahrers vermeiden, indem in aktuellen Systemen indirekt aus Bedienvorgängen des Fahrers auf dessen etwaig bestehende Müdigkeit geschlossen und dem Fahrer dies durch *„sanfte“* Meldun-

---

105 Vgl. *Siebenpfeiffer*: Vernetztes Automobil, 2014, S. 173.

106 Das ABS soll beim Bremsen ein mögliches Blockieren der Räder verhindern, indem es den Bremsdruck vermindert, vgl. https://de.wikipedia.org/wiki/Antiblockiersystem.

107 Da das System bei den verschiedenen Herstellern unterschiedliche Bezeichnungen hat, wird hier stellvertretend von der Bezeichnung „*Antriebsschlupfregelung*“ ausgegangen. Die ASR verhindert ein Durchdrehen der Räder und ein seitliches Ausbrechen des Kraftfahrzeugs beim Anfahren mit viel Gas oder bei schlechtem Untergrund wie Eis oder Rollsplitt, vgl. https://de.wikipedia.org/wiki/Antriebsschlupfregelung.

108 Durch gezieltes Abbremsen einzelner Räder wird durch das ESP als Erweiterung und Verknüpfung des ABS mit einer ASR und einer Elektronischen Bremskraftverstärkung dem Ausbrechen des Kraftfahrzeugs entgegengewirkt, vgl. https://de.wikipedia.org/wiki/Fahrdynamikregelung.

109 Vgl. *Reif*: Bosch Autoelektrik und Autoelektronik, ^{6}2011, S. 338.

gen signalisiert wird.[110] Dieses Fahrerassistenzsystem erzeugt Daten, die Rückschlüsse auf den Fahrer, sein Fahrverhalten und seine körperliche Verfassung zulassen. Dies erscheint bedenklich, sodass hier die datenschutzrechtliche Relevanz in jedem Fall gegeben ist.

Die ***Berganfahrhilfe*** wird auch als *„Hill Hold Control"* oder *„Rückrollsperre"* bezeichnet. Durch den Hill Hold-Sensor wird registriert, dass das Kraftfahrzeug am Berg automatisch gehalten wird. Dies kann auf übermäßige Bremsbeanspruchung hinweisen und zu erkennen geben, ob das Kraftfahrzeug in unwegsamem Gelände gefahren wurde. Letztlich handelt es sich aber lediglich um eine Komfortfunktion für den Fahrer.[111]

Bei der ***Einparkhilfe*** wird durch Ultraschallsensoren und Kameras der Abstand zu Hindernissen vor, hinter und teilweise seitlich des Kraftfahrzeugs optisch oder akustisch angezeigt.[112] Es sind Rückschlüsse darauf möglich, ob der Fahrer oft sehr eng parkt und dadurch Risikobereitschaft zeigt. Die Daten sind mithin für den Fahrer relevant.

In der technischen Entwicklung befindet sich derzeit auch die kamerabasierte ***Fußgängerdetektion***. Dabei wird unterschieden zwischen videobildbasierten Verfahren für den Tag und infrarotbasierten Verfahren für die Nacht.[113] Die im Kraftfahrzeug nach vorne gerichtete Kamera registriert dabei menschliche Umrisse und stellt diese auf dem Kamerabildschirm dar. Auf den Fahrer ist diese Kamera zwar nicht gerichtet. Die dadurch erzeugten Daten sind allerdings für Dritte, die dort abgebildet werden, relevant.

Beim ***Nachtsichtassistent*** gilt ähnliches wie bei vorgenannter Fußgängerdetektion. Er bietet als optisches System aber eine höhere Sichtweite in der Dunkelheit durch Anwendung von Infrarotlicht.[114] Auch dabei können Daten erzeugt werden, vor denen der Fahrer zu schützen ist. Mithin muss auch hierbei die Relevanz der Daten beachtet werden.

---

110 Teilweise soll eine etwaige Müdigkeit durch Überwachung der Einhaltung der Spur zwischen Fahrbahnmarkierungen durch Auswertung von Bildern der Videokamera, teilweise durch laufende, feinfühlige Überwachung der Lenkbewegungen erkannt werden, vgl. https://de.wikipedia.org/wiki/Aufmerksamkeits-Assistent.

111 Vgl. https://de.wikipedia.org/wiki/Berganfahrhilfe.

112 Bei dem sog. Parklenkassistenten, der durch Knopfdruck aktiviert werden kann, führt das Kraftfahrzeug die Lenkmanöver sogar selbständig durch, vgl. https://de.wikipedia.org/wiki/Einparkhilfe.

113 Vgl. *Winner/Hakuli/Wolf*: Handbuch Fahrerassistenzsysteme, ^{2}2012, S. 223.

114 Vgl. https://de.wikipedia.org/wiki/Nachtsicht-Assistent.

Das ***Rückfahrsystem*** bietet Unterstützung beim Rückwärtsfahren und beseitigt den toten Winkel, indem Bilder von einer Heckkamera aufgenommen und zu einem Monitor beim Fahrer übertragen werden.[115] Auch hierbei können die erzeugten Daten für den Fahrer relevant werden. Rückschlüsse aus verkehrsrechtswidrigem Verhalten lassen sich ohne weiteres ziehen.

Eine weitere Gruppe von Fahrerassistenzsystemen in diesem Bereich ist die *der* ***Spurerkennungs- und Spurhaltesysteme***. Das Spurerkennungssystem auf Basis eines Bildverarbeitungssystems warnt[116] allgemein vor dem Verlassen der Fahrspur und ist jeweils in den nachfolgend thematisierten Spurhaltesystemen enthalten. Der Spurassistent registriert dabei ein unbeabsichtigtes Verlassen des Fahrstreifens.[117] Varianten dieser Art von Fahrerassistenzsystemen sind der Spurhalteassistent und die Spurhalteunterstützung[118], der Spurwechselassistent[119] sowie die Spurwechselunterstützung[120]. Das Eingreifen der Spurhalteassistenten lässt Rückschlüsse darauf zu, ob der Fahrer möglicherweise sein Kraftfahrzeug nicht ordnungsgemäß lenkt, verkehrswidrig oder verkehrsgefährdend fährt. Diese Daten könnten von Seiten des Herstellers, der Versicherung oder gar des Flottenbetreibers gegen ihn verwendet werden.

Zuletzt sei in diesem Zusammenhang die ***Verkehrszeichenerkennung*** genannt. Dieses System arbeitet mit einer nach vorne gerichteten Kamera und kann durch Verfahren der Bilderkennung Verkehrszeichen erkennen und diese dem Fahrer anzeigen. Dies allein erzeugt jedoch keine relevanten Daten.[121]

---

115 Vgl. https://de.wikipedia.org/wiki/Rückfahrsystem.

116 Eine Alarmierung erfolgt optisch, akustisch oder haptisch, vgl. https://de.wikipedia.org/wiki/Fahrspurerkennung.

117 Vgl. *Pfeffer/Harrer*: Lenkungshandbuch, ^{2}2013, S. 460.

118 Der Spurhalteassistent, „*Lane Departure Warning*“ (LDW), ermittelt über optische Systeme die Position des Fahrzeugs in der Fahrspur und warnt vor Verlassen derselben, während die Spurhalteunterstützung, „*Lane Keeping Support*“ (LKS), den Fahrer durch automatisiertes permanentes Mitlenken unterstützt, vgl. https://de.wikipedia.org/wiki/Spurhalteassistent.

119 Dabei erfolgt eine Warnung des Fahrers vor drohenden Kollisionen beim Spurwechsel, indem mittels Radar, Kamera oder Laser herannahende Fahrzeuge ermittelt werden, vgl. https://de.wikipedia.org/wiki/Spurwechselassistent.

120 Die Spurwechselunterstützung, „*Lane Change Support*“ (LCS) ist eine Weiterentwicklung zur Spurwechselassistenz und kann auf Wunsch des Fahrers einen automatischen Spurwechsel durchführen, vgl. https://de.wikipedia.org/wiki/Spurwechselassistent.

121 Durch Verknüpfung mit anderen Daten können jedoch relevante Daten generiert werden, vgl. dazu unter *Kapitel 2, Teil 5, II.*.

2. Bremsen

Für den Teilbereich *„Bremsen“* existieren ***Bremsassistenten***[122] und ***Notbremsassistenten***[123]. Beide unterscheiden sich darin, dass der Bremsassistent vom Fahrer aktiv eingeschaltet wird, während der Notbremsassistent eine vom Bordcomputer des Kraftfahrzeugs initiierte Bremsung durchführt.[124] Letzterer stellt ein sog. *„intelligentes“* Sicherheitssystem dar, bei dem Hindernisse via Radar oder Lidar erkannt werden können.[125] Aus den erzeugten Daten, die den Bremsvorgang einleiten, lässt sich jedoch nicht erkennen, warum der Abstand zum Vordermann so gering war, dass ein Bremsvorgang eingeleitet werden musste. Ein direkter Rückschluss auf fehlerhaftes Fahrverhalten ist zwar dadurch nicht möglich. Allerdings müsste zunächst von einem zu geringen Sicherheitsabstand ausgegangen werden, sodass die Relevanz letztlich doch gegeben ist.

Bei der ***Auffahrwarnung*** wird der Fahrer zunächst durch optische oder akustische Signale gewarnt, wobei das System bei Missachtung der Warnung selbständig einen Bremsvorgang einleitet.[126] Auch aus den daraus generierten Daten wäre ein Rückschluss auf verkehrswidriges Verhalten möglich.

3. Abstand

Durch den ***Abstandsregeltempomat***[127] werden Position und Geschwindigkeit des vorausfahrenden Kraftfahrzeugs per Sensor ermittelt und Geschwindigkeit sowie Abstand des eigenen Kraftfahrzeugs entsprechend adaptiv mit Motor- und Bremseingriff angepasst.[128]

---

122 Der Einbau von Bremsassistenzsystemen ist nunmehr verpflichtend vorgeschrieben, vgl. dazu *Verordnung (EG) Nr. 78/2009 des Europäischen Parlaments und des Rates vom 14. Januar 2009 über die Typgenehmigung von Kraftfahrzeugen im Hinblick auf den Schutz von Fußgängern und anderen ungeschützten Verkehrsteilnehmern, zur Änderung der Richtlinie 2007/46/EG und zur Aufhebung der Richtlinien 2003/102/EG und 2005/66/EG vom 14.01.2009*, ABl. Nr. L 35 vom 04.02.2009, S. 1. Die zeitliche Umsetzung ist in Art. 9 VO (EG) 78/2009 geregelt.

123 Gesetzlich verpflichtend ist auch der Einbau solcher Systeme vorgeschrieben, vgl. dazu *Verordnung (EG) Nr. 661/2009 des Europäischen Parlaments und des Rates vom 13. Juli 2009 über die Typgenehmigung von Kraftfahrzeugen, Kraftfahrzeuganhängern und von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge hinsichtlich ihrer allgemeinen Sicherheit vom 13.07.2009*, ABL. Nr. L vom 31.07.2009, S. 1.

124 Vgl. https://de.wikipedia.org/wiki/Bremsassistent.

125 Vgl. https://de.wikipedia.org/wiki/Notbremsassistent.

126 So bei Modellen von BMW, vgl. *Gulde*, Auto Motor und Sport (26/2013), S. 106-108 (108).

127 „*Adaptive Cruise Control*“ (ACC).

128 Vgl. https://de.wikipedia.org/wiki/Abstandsregeltempomat.

Bei dem ***Intelligenten Geschwindigkeitsassistenten*** werden Geschwindigkeitslimits entweder in einer digitalen Karte im Navigationsgerät gespeichert oder durch die bereits erwähnte[129] Verkehrszeichenerkennung ermittelt und die Geschwindigkeit – teilweise auch gegen den Willen des Fahrers – fremdgesteuert.[130]

Der ***Stauassistent*** funktioniert nur auf Autobahnen bzw. vergleichbar ausgebauten Straßen und nur bis zu einer Geschwindigkeit von 40 km/h und ermöglicht durch eine Kombination aus Abstandstempomat und nach vorn gerichteter Kamera, dass das Kraftfahrzeug selbständig den Abstand zum vorausfahrenden Kraftfahrzeug konstant hält, bremst, wieder anfährt und selbständig lenkt.[131] Durch alle diese Systeme wird die Fahrleistung des Fahrers beeinflusst und dieser unterstützt. Allerdings wird dadurch auch erkennbar, ob der Fahrer beispielsweise den gesetzlich vorgesehenen Mindestabstand einhält bzw. ob er häufig den vom System gewählten Abstand durch Übersteuern und Treten des Gaspedals selbständig verringert. Deshalb ist diesbezüglich eine datenschutzrechtliche Relevanz gegeben.

4. Kommunikation und Navigation

Mittlerweile hat auch die Kommunikation in sämtlichen Formen Einzug in das Kraftfahrzeug gehalten. Das Mobiltelefon kann heutzutage entweder fest eingebaut oder aber über eine Drahtlosverbindung und mittels Freisprecheinrichtung mit dem Kraftfahrzeug verbunden sein. Wenn ein Mobiltelefon drahtlos per Bluetooth an das Kraftfahrzeug gekoppelt ist, werden die Kontakte des Besitzers bei manchen Modellen auf das Kraftfahrzeug übertragen und bleiben teilweise auch für den Fall des Verkaufs des Kraftfahrzeugs dort. Dies ist im Hinblick auf den Datenschutz höchst bedenklich und relevant. Im Bereich der Navigation wird der Fokus immer mehr auf sog. Augmented-Navigation-Lösungen[132] gelegt. Dabei ergänzen aktuelle Verkehrsdaten aus dem Internet die Navigationsdaten mit der Folge, dass zukünftig aktuelle Daten über Baustellen oder Staus übermittelt werden können.[133]

---

129 Vgl. unter *Kapitel 2, Teil 3, II.1.*.

130 Vgl. https://de.wikipedia.org/wiki/Intelligent_Speed_Adaption.

131 So bei Modellen von BMW, vgl. *Gulde*, Auto Motor und Sport (26/2013), S. 106-108 (108).

132 Da es sich dabei um Telematik-Anwendungen handelt, wird dies im Laufe der weiteren Bearbeitung nochmals aufgegriffen werden, vgl. unter *Kapitel 2, Teil 4, II.1.*.

133 Vgl. http://www.springerprofessional.de/wie-das-internet--das-auto-revolutioniert/4997584.html.

Teil 4: Datenerzeugung durch den Einsatz von Telematik

Heutzutage kommt im Zusammenhang mit der zunehmenden Vernetzung von Kraftfahrzeugen aber auch der sog. Verkehrstelematik eine entscheidende Rolle zu.

I. Verkehrstelematik und die Connected Car-Technologie

Die Verkehrstelematik ist eine Sonderform der Telematik[134] im Bereich des Straßenverkehrs.

> *„Unter Verkehrstelematik werden Informations- und Kommunikationssysteme verstanden, die dynamische Daten aus Verkehrsmitteln und Verkehrssystemen sammeln, strukturiert aufbereiten und öffentlichen Institutionen, privaten Unternehmen sowie privaten Nutzern zur Verfügung stellen, um Fahrzeugbewegungen und Verkehrsströme zu beeinflussen.“*[135]

Dies ist ein Instrument zur Integration von Informations-, Kommunikations- und Leittechniken, um den Verkehr von Personen und Gütern effizienter, sicherer und umweltfreundlicher zu gestalten.[136] Sie dient dem Verkehrsmanagement und erfordert dazu ein Zusammenwirken von verschiedenen Systemen zur Verkehrserfassung.[137] Zukünftig sollen Daten auch über kooperative Systeme zwischen einzelnen Kraftfahrzeugen ausgetauscht werden, indem die im Kraftfahrzeug vorhandenen Daten erfasst und zu einem Zentralrechner geschickt werden, der eine Fahrempfehlung ermittelt und diese dem Fahrer übermittelt.[138] Als Übertragungswege stehen sowohl Rundfunk als auch Mobilfunk-

---

134 Telematik ist *„das Mittel der Informationsverknüpfung von mindestens zwei Informationssystemen mit Hilfe eines Telekommunikationssystems, sowie einer speziellen Datenverarbeitung“*, vgl. Definition von *Nora/Minc*: L`informatisation de la société: rapport à M. le Président de la République 1978, zitiert nach Wikipedia: https://de.wikipedia.org/wiki/Telematik.

135 Vgl. *Klaus/Krieger*: Gabler-Lexikon Logistik - Management logistischer Netzwerke und Flüsse (A-Z), [4]2008, Stichwort "*Telematik*", S. 564.

136 Vgl. Empfehlungen des 35. Deutschen Verkehrsgerichtstages 1997, http://www.deutscher-verkehrsgerichtstag.de/images/empfehlungen_pdf/empfehlungen_35_vgt.pdf..

137 Dazu zählen z.B. Parkleitsysteme, Knotenpunkt- oder Streckenbeeinflussungsanlagen, vgl. *Boltze/Wolfermann*: Leitfaden Verkehrstelematik, 2006, S. 22 und 32.

138 Vgl. https://de.wikipedia.org/wiki/Verkehrstelematik.

netze zur Verfügung.[139] Mittlerweile wird der allgemeine Begriff der Telematik jedoch durch den Begriff des *„Intelligent Transport System"* (ITS) mehr und mehr ersetzt.[140]

Die sog. Connected Car-Technologie stellt wiederum einen Spezialfall der Verkehrstelematik dar. Dabei wird als Übertragungsweg zum Austausch von Informationen zwischen Kraftfahrzeugen untereinander oder vom Kraftfahrzeug zu straßenseitig installierten Einheiten der Einsatz von drahtlosen ad-hoc-Netzwerken nach dem WLAN[141]-Standard angestrebt.[142] Diese sog. Car to X-Kommunikation[143] führt dazu, dass Kraftfahrzeuge außer *„fühlen"* und *„sehen"* nunmehr auch *„hören"* können.[144] Das Kraftfahrzeug wird dabei derart vernetzt, dass es mit anderen Kraftfahrzeugen und der Umwelt kommunizieren kann. Deshalb kann man dies als integrales Sicherheitssystem bezeichnen, bei dem Umfelddaten aus Sensoren in Kombination mit den Daten aus Car to X dazu genutzt werden können, um *„um die Ecke"* zu schauen und potenzielle Unfallgegner zu erkennen.[145] Die Kraftfahrzeuge kommunizieren untereinander und tauschen Informationen über Staus oder Straßenverhältnisse aus, die dann jedem einzelnen Fahrer zur Verfügung gestellt werden.

II. Datenerzeugung

Im Zusammenhang mit der Verkehrstelematik und der Connected Car-Technologie sind verschiedene Arten von Daten zu unterscheiden, so z.B. Verkehrs- und Umfelddaten sowie sonstige Daten.[146] Die Daten können künftig[147] mit der offenen und systemunabhängigen Telematikplattform *„Openmatics"* innerhalb einer einzigen On-Board-Unit

---

139 Beim analogen FM-Rundfunk (UKW) wird zur Übertragung von Verkehrsnachrichten in einen Traffic Message Channel (TMC) das Radio Data System (RDS) verwendet, während beim digitalen Rundfunkverfahren das Digital Audio Broadcast (DAB) hinzukommt; über das Mobilfunknetz können individuelle Nachrichten auch aus dem Auto heraus an eine Dienstzentrale im Wege des Short Message Services (SMS) oder dem General Packet Radio Service (GPRS) übertragen werden, vgl. *Reif*: Fahrstabilisierungssysteme und Fahrerassistenzsysteme, 2010, S. 201.

140 Vgl. *Funken/Schulz-Schaeffer*: Digitalisierung der Arbeitswelt, 2008, S. 72.

141 „*Wireless local area network*".

142 Vgl. *Reif*: Fahrstabilisierungssysteme und Fahrerassistenzsysteme, 2010, S. 201 f..

143 Vgl. unter *Kapitel 2, Teil 4, II.4.*.

144 Vgl. VDA Jahresbericht 2014, S. 163, https://www.vda.de/de/services/Publikationen/jahresbericht-2014.html.

145 Vgl. *Franke/Gonter/Leschke/Kücukay*, ATZ 2012, S. 918-923 (919).

146 Verkehrsdaten sind Infrastrukturdaten, wie z.B. die Fahrstreifenzuordnung, während Umfelddaten z.B. die Niederschlagsmenge oder Temperatur betreffen; unter den sonstigen Daten versteht man Störmeldungen oder Informationen über Baustellen, vgl. *Boltze/Wolfermann*: Leitfaden Verkehrstelematik, 2006, S. 92.

147 Zum jetzigen Zeitpunkt sind die meisten Telematik-Systeme nur für einen speziellen Dienst entwickelt, sodass für jeden Dienst eine Telematik-Box notwendig ist. Auf diese Unterscheidung kommt es aber für die Untersuchung nicht weiter an.

(OBU) erfasst und versendet werden, wobei die Auswertung der Informationen auf einem webgestützten Portal erfolgt.[148] Problematisch im gesamten Bereich der Car to X-Kommunikation sind jedoch die Gefahren, die im Hinblick auf die dadurch erzeugten Daten entstehen, vor allem durch Manipulation von außen, Abhören oder Übernahme der Kontrolle der Systeme. So ist es denkbar, dass durch einen Angriff auf das System von außen ein Stau künstlich provoziert oder eine durchgehende Ortung von Kraftfahrzeugen möglich gemacht werden könnte.[149] Insoweit kann jede Art von Car-to-X-Kommunikation im Ergebnis zur Verarbeitung datenschutzrelevanter Daten führen, sodass im Rahmen der rechtlichen Betrachtung die Zugriffsbefugnis für solche Daten geklärt werden muss.

1. Fahrzeugintern durch Telematik-Anwendung

Fahrzeugintern wird es im Bereich der Telematik zunehmend darauf ankommen, sog. Infotainment-Angebote im Kraftfahrzeug zu integrieren. Zum einen kann dies durch eigene Premiumdienste des Herstellers gelingen[150], zum anderen aber auch über die Möglichkeit, sog. *„Smart Devices"*[151] mit dem Bordcomputer zu verbinden. Auch bei den Telematik-Anwendungen kann zwischen nutzerbezogener und fahrzeugbezogener Telematik unterschieden werden.[152] Die Navigation als Beispiel nutzerbezogener Telematik kann so ausgestaltet sein, dass alle Teilaufgaben der Navigation, wie z.B. Ortung, Routensuche und Zielführung, im Kraftfahrzeug selbst erbracht werden. Dies erfolgt durch die Sensorik zur Positionsbestimmung.[153]

---

148 Dadurch dass das System herstellerunabhängig funktioniert, können z.B. auch Drittanbieter eigene Apps programmieren und auf dem Portal zum Download anbieten, vgl. *Siebenpfeiffer*: Vernetztes Automobil, 2014, S. 168 f..

149 Vgl. http://winfwiki.wi-fom.de/index.php/Gefahrenanalyse_Connected_Cars.

150 Angebote gibt es in diesem Bereich z.B. von BMW in Gestalt des „*Connected Drive Services*", wodurch unter anderem auch Apps in das Kraftfahrzeug integriert werden können, vgl. http://www.bmw.de/de/topics/faszination-bmw/connecteddrive-2013/services-apps/connecteddrive-services.html.

151 Ein Mobiltelefon stellt ein Smart Device dar. Als Smart Device bezeichnet man informationstechnisch aufgerüstete Alltagsgegenstände, die einen Mehrwert durch sensorgestützte Informationsverarbeitung und Kommunikation erhalten, vgl. *Roberts*: Gabler-Wirtschafts-Lexikon, Band Sl-U, [17]2010, Stichwort "*Smart Device*", S. 2732.

152 Zu nutzerbezogener Telematik gehören die Navigation und die Einbindung des Telefons in die Kommunikations- und Unterhaltungstechnik des Kraftfahrzeugs, während der integrierte Notruf und die Anzeige von Tankstellen sowie das automatische Buchen fälliger Service-Termine fahrzeugbezogenen sind, vgl. *Wallentowitz*: Handbuch Kraftfahrzeugelektronik, [1]2006, S. 457.

153 Vgl. *Winner/Hakuli/Wolf*: Handbuch Fahrerassistenzsysteme, [2]2012, S. 600. Zur Offboard-Navigation und zur Hybrid-Navigation vgl. unter *Kapitel 2, Teil 4, II.3.*.

Die App[154]-Integration im Kraftfahrzeug schreitet ebenfalls immer weiter voran. Es gibt bereits Systeme, die zwischen dem mobilen Endgerät des Fahrers und dem fahrzeugseitigen Infotainment-System samt Apps trennen mit der Folge, dass über eine App-Programmierschnittstelle[155] nach der erstmaligen Verbindungsherstellung via Bluetooth Fahrzeugdaten in alle Richtungen übermittelt werden können.[156] Über die App-Integration im Kraftfahrzeug können schließlich auch Daten aus sozialen Netzwerken, wie z.B. Facebook, über die jeweiligen Apps übermittelt und über das Kraftfahrzeug bedient werden.[157] Die Übermittlung solcher Daten ist für den Fahrer auch relevant. Zwar geschieht dies zunächst nur intern. Aber auch Hersteller und Werkstätten haben ein Interesse an solchen Daten, um dem Fahrer beispielsweise auf seine aktuellen Bedürfnisse zugeschnittene Services anbieten zu können. Noch weiter gehen gemeinsame Überlegungen von Apple und BMW. Es kommt die Frage auf, wie man das Apple-Betriebssystem in den BMW i3 integrieren könnte und ob tatsächlich von BMW das sog. Apple-Car gebaut werden wird, wodurch sich BMW einen erheblichen Imageschub dafür erhofft, dass im Gegenzug an Apple geheime Daten des Antriebsmanagements offengelegt werden müssten.[158] Dieses Szenario ist bislang nicht Realität, bleibt aber weiter zu beobachten. Für den Fahrer würde eine solche Verbindung nur noch weitergehende Gefahr für seine Daten bedeuten.

2. Car to Car

Bei der Kommunikation von Kraftfahrzeugen untereinander kann zwischen verschiedenen Szenarien unterschieden werden. Unterhaltungsszenarien können z.B. Telefonieren, Chat-Anwendungen und das Versenden von Kurzmitteilungen zwischen verschiedenen Kraftahrzeugen darstellen, während als sicherheitsrelevante Szenarien die Warnung der anderen Verkehrsteilnehmer vor Staus mit Hinweisen zur Verkehrsleitung und potenziellen Gefahrenquellen, wie z.B. glatten Straßen einzuordnen sind.[159] Gerät ein Kraftfahrzeug beispielsweise in einen Stau, wird dies vom Navigationsgerät erkannt und über den Bordcomputer eine aktuelle lokale Verkehrsmeldung über WLAN an die anderen in

---

154 „*Application Software*“ (Anwendungssoftware).

155 Beim Hersteller Ford wird diese beispielsweise als „*Application Programming Interface*“ (API) bezeichnet, vgl. https://developer.ford.com/tag/api.

156 Vgl. *Pulathaneli*, ATZ elektronik 2014, S. 12-17 (12).

157 Vgl. http://www.faz.net/aktuell/technik-motor/computer-internet/twitter-und-facebook-im-auto-muss-der-autofahrer-sozial-vernetzt-sein-11513198-p2.html.

158 Vgl. http://www.n-tv.de/auto/Baut-BMW-das-Apple-Car-article14646181.html.

159 Vgl. *Winner/Hakuli/Wolf*: Handbuch Fahrerassistenzsysteme, ^{2}2012, S. 617.

der Nähe befindlichen Kraftfahrzeuge übermittelt.[160] Allerdings können durch die mobile Kommunikation mit anderen Kraftfahrzeugen über Chat oder das Versenden von Kurzmitteilungen persönliche Daten des Fahrers übermittelt werden, für die ein vielseitiges Interesse bestehen dürfte.

3. Car to Infrastructure

Hierbei kann unterschieden werden zwischen Aspekten der Unterhaltungsbranche und solchen der Verkehrssicherheit. Ein Unterhaltungsszenario in diesem Bereich ist z.B. der Datendownload von Musik in das Kraftfahrzeug, wohingegen sicherheitsrelevante Szenarien u.a. in der Kommunikation des Kraftfahrzeugs mit Elementen der Verkehrsinfrastruktur (Ampeln, Verkehrsschilder) und der Versendung von Diagnoseinformationen anderer Kraftfahrzeuge zu sehen sind.[161] Die Car to Infrastructure-Kommunikation dient neben Sicherheitsaspekten vor allem auch der Kapazitätssteigerung von Straßen.

Der Empfang von Daten über Ampelzustände, von Verkehrszeichen, Straßenzustand oder über freie Parkplätze wird durch die Kommunikation mit der Infrastruktur durch sog. Roadside Units (RSU) ermöglicht.[162] Dies führt allerdings dazu, dass die dabei generierten Daten im Zweifel auch gegen den Fahrer einsetzbar sind und ihm z.B. ein Rotlichtverstoß nachgewiesen werden könnte. Diese Daten sind mithin wiederum relevant.

In den Bereich der Car-to-Infrastructure-Kommunikation fällt auch das telematische LKW-Parken. Dadurch sollen vorhandene Parkkapazitäten optimal ausgenutzt, der LKW-Verkehr gleichmäßig verteilt und Suchverkehr vermieden werden.[163] Das Anbieten bzw. Übermitteln der Daten erfolgt mittels des sog. Mobilitäts Daten Marktplatzes (MDM), von wo die Daten über TMC an die LKW übertragen werden.[164]

Ebenfalls hierunter fällt die bereits soeben erwähnte Kommunikation zwischen Kraftfahrzeug und Verkehrsbeeinflussungsanlagen jeglicher Art. Dabei werden nach automatischer Datenerhebung mit rechnergesteuerten Hinweisen oder mit verbindlichen An-

---

160 Vgl. http://winfwiki.wi-fom.de/index.php/Standards_in_der_Car-To-Car-Kommunikation.

161 Vgl. *Winner/Hakuli/Wolf*: Handbuch Fahrerassistenzsysteme, [2]2012, S. 617.

162 Dabei senden die Kraftfahrzeuge in kurzen Abständen Statusnachrichten an die RSU, die diese auswertet, sodass die Kraftfahrzeuge daraufhin Informationen über Ampelzustände etc. empfangen können, vgl. http://winfwiki.wi-fom.de/index.php/Standards_in_der_Car-To-Car-Kommunikation.

163 Vgl. http://www.forschungsinformationssystem.de/servlet/is/340039/.

164 Vgl. https://www.bmvi.de/SharedDocs/DE/Anlage/VerkehrUndMobilitaet/Strasse/ivs-telematisches-lkw-parken.pdf?__blob=publicationFile.

ordnungen, über Verkehrszeichenbrücken mit Matrix-Zeichen Folgerungen aus Verkehrsdichte, Fahrbahnzustand und Witterungsverhältnisse gezogen.[165] Auch durch das sog. Floating-Car-Data-Prinzip werden Verkehrsinformationen erfasst, indem das Kraftfahrzeug im Verkehrsstrom zyklisch seine Position und Geschwindigkeit in eine Zentrale überträgt, wo durch statistische Auswertung dieser Daten aktuelle Meldungen über die Verkehrssituation generiert werden.[166] Im Navigationsbereich wird an dieser Stelle die sog. Hybrid-Navigation relevant. Dabei wird für die Navigationsfunktionen auf eine Vielzahl von Datenquellen zurückgegriffen, um beispielsweise die sog. Points of Interest (POI)[167] oder die Kartendaten dynamisch zu aktualisieren, sofern letztere serverbasiert, d.h. außerhalb des Kraftfahrzeugs berechnet werden.[168] Insoweit können Navigationsdaten in Zukunft mit aktuellen Verkehrsdaten aus dem Internet ergänzt werden (sog. Augmented-Navigation-Lösung[169]).[170] Die Relevanz der daraus generierten Daten ist offensichtlich. Die POI werden genau auf den Fahrer abgestimmt. Es werden dafür verschiedenste persönliche Interessen des Fahrers relevant, die in die Auswertung mit einfließen und die vom Fahrer auch selbst im Navigationsgerät gespeichert werden können.

4. Car to X

Unter Car to X-Kommunikation[171] sind sämtliche anderen Kommunikationsformen zwischen dem Kraftfahrzeug und anderen Bereichen zusammenzufassen. Im Flottenmanagement besteht beim Vorhandensein eines ab Werk eingebauten Telematik-Bordmoduls die Möglichkeit, Fahrzeugdaten in Echtzeit und über eine Funkverbindung an den Disponenten zu senden, sodass diesem sämtliche technische Messdaten, wie z.B. die Durchschnittsgeschwindigkeit und die Fahrtstrecke, zur Verfügung stehen.[172] Eine Fernwartung des Kraftfahrzeugs durch damit beauftragte Werkstätten wird hierdurch

---

165 Vgl. *Bouska*, DAR 1995, S. 353-356 (354).

166 Allerdings ist bisher die dazu erforderliche Ausrüstung der Kraftfahrzeuge mit einer Ortungs- und Sendevorrichtung noch nicht ausgereift, vgl. *Reif*: Fahrstabilisierungssysteme und Fahrerassistenzsysteme, 2010, S. 203.

167 Als POI gilt ein Ort, der für den Nutzer eines Navigationsgeräts z.B. zur Befriedigung reisespezifischer oder alltäglicher Bedürfnisse interessant sein kann, vgl. https://de.wikipedia.org/wiki/Point_of_Interest.

168 Vgl. *Winner/Hakuli/Wolf*: Handbuch Fahrerassistenzsysteme, ^{2}2012, S. 609 f..

169 Dabei werden live aufgenommene Videobilder mit zwei- oder dreidimensionalen Navigationsanweisungen kombiniert, vgl. *Shen*, ATZ 2013, S. 402-405 (403).

170 Vgl. http://www.springerprofessional.de/wie-das-internet--das-auto-revolutioniert/4997584.html.

171 Die Kategorie der sog. Car to Pedestrian-Kommunikation wird nicht weiter thematisiert. Darunter fällt die Kommunikation zwischen Fahrzeugsystemen und Mobiltelefonen von Fußgängern, um dadurch im Ergebnis den Fußgängerschutz zu erhöhen, vgl. *Schulz/Roßnagel/David*, ZD 2012, S. 510–515 (510).

172 Vgl. http://winfwiki.wi-fom.de/index.php/Connected_Cars_im_Bereich_der_Flottennavigation.

ebenso ermöglicht, wie die Kommunikation zwischen Kraftfahrzeug und kommerzieller Infrastruktur, wozu Tankstellen, Hotels, Parkhäuser und andere POI zählen.[173] Da diese Daten auf die Wünsche des Fahrers abgestimmt sind bzw. auf dessen Verhalten beruhen, muss hier ebenfalls eine Relevanz der Daten bejaht werden.

5. Forschungsprojekt zum Thema Telematik: simTD

Dass die Verkehrstelematik sämtliche Fachbereiche betrifft und zur Forschung anregt, zeigt die Tatsache, dass mittlerweile verschiedenste Projekte dazu ins Leben gerufen wurden. Das Projekt *„Sichere Intelligente Mobilität – Testfeld Deutschland“* (simTD)[174] ist ein Gemeinschaftsprojekt führender deutscher Automobilhersteller, Automobilzulieferer, Kommunikationsunternehmen und Forschungsinstitute.[175] Alle zur Car to X-Kommunikation gehörenden Technologien und Anwendungen[176] konnten über vier Jahre in einem Versuchsgebiet im Ballungsraum Frankfurt am Main in mehreren hundert Testfahrzeugen – ausgestattet mit Kommunikationseinheiten *(„ITS Vehicle Stations“)* – im alltagsnahen Betrieb untersucht werden.[177] Der Feldversuch hat gezeigt, dass durch die Einführung der Car to X-Kommunikation die Fahr- und Verkehrssicherheit durch Unfallvermeidung und Verbesserung von Reisezeiten erheblich gesteigert werden konnte, sodass damit auch die Praxistauglichkeit der Car to X-Kommunikation bewiesen wurde.[178] Die Versuchsfahrer berichteten von einem erhöhten Sicherheitsgefühl durch Funktionen wie Einsatzfahrzeugwarnung und Querverkehrsassistent, woraus letztlich die Konsequenz gezogen wurde, dass nunmehr als erste Anwendung die Baustellenwarnung in Verbindung mit der Verkehrslageerfassung im Umfeld von Baustellen im *„Cooperative ITS Corridor Rotterdam – Frankfurt am Main – Wien“* realisiert werden soll.[179]

---

173 Vgl. http://winfwiki.wi-fom.de/index.php/Connected_Cars_-_Angriffsszenarien_und_m%C3%B6gliche_Folgen.

174 Aufgrund der Vielzahl an Projekten dieser Art soll hier einzig das Projekt simTD dargestellt werden.

175 Vgl. ZD-Aktuell 2012, 03056.

176 Dazu gehören Funktionen wie Baustelleninformationen, Warnung vor Einsatzfahrzeugen, Ampelphasen-Assistent, lokale verkehrsabhängige Lichtsignalanlagensteuerung und Standortinformationsdienste, vgl. http://www.simtd.de/index.dhtml/object.media/deDE/7228/CS/-/news/Presse/simTD_Pressemitteilung_11-10-2011_DE.pdf.

177 Vgl. http://www.simtd.de/index.dhtml/object.media/deDE/5907/CS/-/news/Presse/simTD_PM01.pdf.

178 Vgl. http://www.simtd.de/index.dhtml/object.media/deDE/8033/CS/-/news/Presse/simTD-Pressemitteilung_2013_DE.pdf.

179 Vgl. http://www.simtd.de/index.dhtml/object.media/deDE/8022/CS/-/backup_publications/Informationsmaterial/simTD_prsentation_2013_de_web.pdf.

Teil 5: Datenerzeugung durch Big Data-Anwendung

Mittlerweile gibt es aber auch eine letzte Kategorie, die für die Datenerzeugung im Kraftfahrzeug eine immer größere Rolle spielt. Diese betrifft die sog. Big Data-Anwendungen. Kraftfahrzeug, Kunde, Umgebung, Werkstatt und Hersteller werden künftig online über die Cloud verbunden sein, wenn die übermittelten Daten pro Fahrzeug in den nächsten Jahren im Monat von circa 4 Megabyte auf 5 Gigabyte anwachsen werden.[180]

I. Big Data - ein Überblick

Big Data bezeichnet die Analyse großer Datenmengen aus vielfältigen Quellen mit einer hohen Verarbeitungsgeschwindigkeit zur Erzeugung wirtschaftlichen Nutzens.[181] Gemeint ist dabei die technologische Fähigkeit, sehr große, scheinbar ungeordnete und heterogene Datenmengen, die für sich gesehen wert- und sinnlos erscheinen, in einer relativ kurzen Zeit so zu messen, zu verknüpfen und aufzubereiten, dass daraus nutzbare neue Erkenntnisse gewonnen werden können.[182] Durch die Sichtung der Daten auf zunächst nicht sichtbare Muster und Strukturen gewinnen die Daten einen neuen Aussagegehalt und es werden letztlich neue Daten dadurch geschaffen, dass der vorhandenen Datenmasse neue Informationen entnommen werden.[183]

Im Zusammenhang mit vernetzten Kraftfahrzeugen meint die Anwendung von Big Data, dass die einzelnen verschiedensten im Kraftfahrzeug anfallenden Daten[184] derart miteinander verknüpft werden, dass durch die Verknüpfung neue Daten erzeugt werden. Der BITKOM-Arbeitskreis *„Big Data“* formuliert dies wie folgt:

> *„Big Data bezeichnet die wirtschaftlich sinnvolle Gewinnung und Nutzung entscheidungsrelevanter Erkenntnisse aus qualitativ vielfältigen und unterschiedlich strukturierten Informationen, die einem schnellen Wandel unterliegen und in bisher ungekanntem Umfang anfallen. Big Data stellt Konzepte, Methoden, Technologien, IT-Architekturen sowie Tools zur Verfügung, um die geradezu*

---

180 Vgl. http://www.springerprofessional.de/big-data-und-cloud-vernetzen-das-auto/4980046.html.

181 Vgl. https://www.bitkom.org/Bitkom/Publikationen/Leitfaden-Big-Data-im-Praxiseinsatz-Szenarien-Beispiele-Effekte.html.

182 So *Hartmann*, DAR 2015, S. 122–126 (122).

183 Vgl. *Zdanowiecki* in Bräutigam/Klindt: Digitalisierte Wirtschaft / Industrie 4.0, S. 20.

184 Vgl. insgesamt die bereits dargestellten erzeugten Daten durch Sensoren, Fahrerassistenzsysteme und Telematik.

exponentiell steigenden Volumina vielfältiger Informationen in besser fundierte und zeitnahe Management-Entscheidungen umzusetzen und so die Innovations- und Wettbewerbsfähigkeit von Unternehmen zu verbessern."[185]

Typisch dabei ist, dass die einzelnen gewonnenen Daten meist für sich gesehen völlig unverfänglich sind, aber es in der Verbindung als Big Data ermöglichen, ein Profil des Fahrers zu erstellen.[186] Bereits im aufsehenerregenden Fall des sog. Autobahnschützen, der im Jahr 2014 vor dem Landgericht Würzburg vor Gericht stand und zu einer Freiheitsstrafe von 10 Jahren verurteilt wurde[187], konnte das Bundeskriminalamtes (BKA) durch Anwendung von Big Data den Täter im Jahr 2013 fassen, der an Autobahnen willkürlich auf vorbeifahrende Autos, meist LKW schoss. Gefunden hat das BKA diese *„Nadel im Heuhaufen"* durch die Sammlung, automatisierte Auswertung und Analyse von gewaltigen Datenbergen.[188] Das Urteil des Landgerichts Würzburg wurde mit Beschluss vom 16.07.2015 vom Bundesgerichtshof weitgehend bestätigt.[189]

Den Vorteilen, die Big Data augenscheinlich zu bieten hat, stehen allerdings die Risiken gegenüber, die insbesondere durch Missbrauch der Datenmengen entstehen könnten.

Besondere Aufmerksamkeit erlangte dabei ein Fall aus den Niederlanden, als bekannt wurde, dass der Navigationsgerätehersteller TomTom anonymisierte Verkehrsbewegungsdaten an die Polizei verkaufte, woraufhin diese ihre Geschwindigkeits- oder sonstigen Verkehrskontrollen effektiver gestalten konnte.[190] Durch die zuständigen Aufsichtsbehörden wurde jedoch ein Jahr später festgestellt, dass die Weitergabe der Daten vollkommen anonym erfolgte und dadurch im Ergebnis keine gesetzlichen Bestimmungen verletzt wurden.[191] Ein Beigeschmack bei diesem Vorgehen bleibt allerdings.

---

185 Vgl. https://www.bitkom.org/Bitkom/Organisation/Gremien/Big-Data.html.

186 Beispielhaft sei der Blinkerhebel-Sensor genannt; an sich erfasst er nur, wann die Blinkerleuchten angesteuert wurden. Verknüpft man die daraus erzeugten Daten allerdings z.B. mit denen der Lenkradbewegung, kann dadurch ein etwaiger Verstoß gegen Verkehrsregeln (Abbiegen ohne zu blinken) nachgewiesen werden, vgl. unter *Kapitel 2, Teil 2, 2.b)*.

187 Vgl. http://www.autobild.de/artikel/autobahnschuetze-urteil-5256042.html.

188 Anhand von Kameras an sieben Autobahnschnittstellen und die dadurch erfolgte Kennzeichenerfassung konnten wahrscheinliche Fahrtstrecken des Schützen analysiert und durch die Bilder der Überwachungskameras ein Verdächtiger ausgemacht sowie daraufhin ein Abgleich der Handy-Funkzelleninformationen vorgenommen werden, vgl. http://www.computerwoche.de/a/problemfall-big-data,2546584.

189 Bundesgerichtshof, Beschluss vom 16.07.2015, Aktenzeichen 4 StR 117/15, NZV 2016, S. 40-41.

190 Vgl. http://www.spiegel.de/netzwelt/gadgets/standortsuche-fuer-radarfallen-tomtom-entschuldigt-sich-fuer-deal-mit-der-polizei-a-759464.html.

191 Vgl. *Kamps*, Internationales Verkehrswesen 2014, S. 18–19 (18).

Aber auch national zeigten sich bereits digitale Sicherheitslücken bei herstellereigenen Premiumdiensten, wie dem Kommunikationssystem *„ConnectedDrive“* von BMW. Ein Experte des ADAC konnte bei einem Versuch das System digital manipulieren, indem er in der Nähe der ConnectedDrive-Modelle eine eigene Mobilfunkstation aufbaute, mit der sich die SIM-Karte des Steuergerätes automatisch verbunden und die Daten nur noch an die gefälschte Basisstation übertragen hatte, wodurch es ihm möglich wurde, das Fahrzeug fernzusteuern und die Fahrertür über die Programmierung *„Fahrertür öffnen“* tatsächlich zu öffnen.[192]

II. Datenerzeugung und mögliche Anwendungsbereiche

Die oben dargestellten Daten aus Sensoren oder Telematik-Anwendungen werden durch die Anwendung von Big Data derart zusammengeführt, dass daraus neue verwertbare Daten entstehen, die von unterschiedlichen Anwendern genutzt werden können.

Beispielsweise[193] kann eine Werkstatt bei Zugriff auf die Daten des Bremsflüssigkeitsstandsensor und gleichzeitiger Vernetzung des Mobiltelefons des Fahrers mit dem Fahrzeug sich mit diesem in Verbindung setzen und einen Wartungstermin vorschlagen. Werden Verschleiß und Fehlerspeicher über die Datenfernverbindung des Mobiltelefons im Kraftfahrzeug ausgelesen, können die nötigen Ersatzteile bereits bestellt oder gar Ferndiagnose und Fernwartung angeboten werden.[194]

Durch sog. GPS-Tracker ist auch die Ortung des Kraftfahrzeugs und im Falle eines Diebstahls auch die Nachverfolgung der Fahrtroute samt Übermittlung des Standorts an den Halter möglich.[195] In Verknüpfung mit Geschwindigkeits-Informationen gibt der GPS-Sensor auch Auskunft über die Fahrweise des Fahrers an reglementierten Stellen, z.B. im Bereich eines Tempolimits. Verknüpft mit dem Regen-Licht-Sensor[196] kann die Information entstehen, dass bei nasser Fahrbahn zu schnell gefahren wurde.

Genauso ist durch Verknüpfung des Videokamera-Systems mit anderen Sensoren die Dokumentation von Tempoüberschreitungen oder Missachtung von Überholverboten denkbar. Durch Verknüpfung des Systems der kamerabasierten Fußgängerdetektion mit

---

192 Vgl. *Kroher*, ADAC Motorwelt (2/2015), S. 20–21 (20).

193 An dieser Stelle können wegen der enormen Vielzahl an Möglichkeiten nur einige nicht abschließende Beispiele aufgeführt werden, um die Brisanz von Big Data-Anwendungen zu demonstrieren.

194 Vgl. *Funke*, blinklicht 2012, S. 10.

195 Vgl. http://www.pcwelt.de/ratgeber/Auto-Diebstahl_Technik_Schutz-8098778.html.

196 Vgl. unter *Kapitel 2, Teil 2, I.1.a)*.

anderen Daten ist rekonstruierbar, ob und warum es zu einem etwaigen Unfall mit Fußgängerbeteiligung kam, was insbesondere für den Fahrer bei der Geltendmachung von Ansprüchen gegen seine Versicherung relevant sein kann.

Durch Verknüpfung der Verkehrszeichenerkennung mit dem Intelligenten Geschwindigkeitsassistenten[197] kann sogar die Fahrgeschwindigkeit automatisch geregelt werden.[198] In diesem Fall lassen die Daten dann ebenfalls einen Rückschluss auf Geschwindigkeitsüberschreitungen zu, wenn der Fahrer dieses System übersteuert. Ein Flottenbetreiber hätte durch Big Data-Anwendung die Möglichkeit, über die Auswertung von Daten des GPS-Sensors und Handyortung jederzeit herauszufinden, wo sich der Mitarbeiter mit dem entsprechenden Firmenfahrzeug befindet. Dies wäre auch unabhängig von der Arbeitszeit und nicht auf einen bestimmten räumlichen Bereich beschränkt.

Damit die Anwendung von Big Data aber weiter Verbreitung finden kann, muss auch die technische Entwicklung Schritt halten. Die Softwareentwicklung für die Verarbeitung von Big Data befindet sich noch im Anfangsstadium und soll derart ausgestaltet werden, dass die Software parallel auf bis zu Hunderten oder Tausenden von Prozessoren bzw. Servern arbeitet.[199]

Die möglichen Anwendungsgebiete für den Einsatz von Big Data sind weitreichend.[200]

Im Bereich *„Distribution und Logistik“* wird Big Data dazu eingesetzt, Lieferketten zu optimieren (sog. Supply Chain Management), Verkehrstelematik zur Verminderung von Stillstandzeiten bei LKW-Transporten zu verhindern und Optimierungen bei der Mauterhebung zu schaffen.[201]

Auch Versicherungen machen sich Datenmengen ihrer Kunden zunutze. Die Sparkassen DirektVersicherung AG führte in der Sparte *„Autoversicherung“* mittlerweile den Tarif *„S-Drive“* als ersten Telematik-Sicherheits-Service ein, bei dem aus den anhand einer im Kraftfahrzeug eingebauten Telematik-Box generierten Daten durch einen beauftragten externen Dienstleister ein Telematik-Score ermittelt und an die Versicherung wei-

197 Vgl. unter *Kapitel 2, Teil 3, II.3.*.
198 Vgl. https://de.wikipedia.org/wiki/Verkehrszeichenerkennung.
199 Vgl. https://de.wikipedia.org/wiki/Big_Data.
200 Aus diesem Grund können hier nicht sämtliche Einsatzmöglichkeiten dargestellt werden. Die Aufzählung ist beispielhaft und nicht abschließend.
201 Vgl. https://www.bitkom.org/Bitkom/Publikationen/Leitfaden-Big-Data-im-Praxiseinsatz-Szenarien-Beispiele-Effekte.html.

tergeben wird, die dem Versicherten bei gutem Gesamtjahres-Scorewert einen Preisnachlass von bis zu 5 % gewährt.[202] Der Versicherer erfährt nach diesem Verfahren nur einen abstrakten Scorewert. Es ist ihm jedoch nicht möglich, die dem zugrundeliegenden Vorgänge im Kraftfahrzeug einzusehen. Grundsätzlich ist es möglich, dieses Modell datenschutzkonform auszugestalten. Dies ist allerdings in der vorgenannten und derzeit durchgeführten Form nicht der Fall, da dadurch einerseits ein massives Überwachungsrisiko besteht, welches sich insbesondere in den Fällen zeigt, in denen wie im Fall der Dienstwagennutzung Fahrer und Versicherungsnehmer nicht personenidentisch sind, und andererseits durch die günstige Preisgestaltung ein ökonomischer Druck erzeugt werden könnte, der Zweifel an der Freiwilligkeit einer erteilten Einwilligung zur Datenverwendung aufkommen lassen könnte.[203]

III. Die Einführung des "eCalls" ab 2018

Die wohl momentan aktuellste Entwicklung im Bereich Big Data ist die für Neufahrzeuge[204] ab 31.03.2018[205] vorgesehene europaweite Einführung des *„Emergency Calls“* (eCall).[206] Es handelt sich dabei um ein System, das im Falle eines Autounfalls automatisch durch den auslösenden Airbag-Sensor und über das Mobilfunknetz die örtlich zuständige Notrufabfragestelle informiert und dorthin ein sog. Minimaldatensatz[207] (*„Minimum Set of Data“*, MSD) mit Hilfe des Satellitennavigationssystems GNSS[208] übertragen sowie eine Sprechverbindung aufgebaut werden.[209] Die Umrüstung der Leitstellen soll dabei von den EU-Staaten finanziert werden.[210] Eine Entschließung des Europäischen Parlaments betonte dazu, dass das eCall-System keinesfalls dazu verwendet werden dürfe, um die Fortbewegung einer Person zu überwachen oder ihren Standort festzustellen, wenn diese nicht in einen Unfall verwickelt ist.[211] Dies verdeutlicht bereits,

---

202 Vgl. https://www.sparkassen-direkt.de/fileadmin/pdf/telematik/folder.pdf.

203 Vgl. *Schwartmann*, Sonderveröffentlichung zu RDV 3/2015, S. 2.

204 Gemeint sind neu typgeprüfte Fahrzeuge. Für Gebrauchtwagen gilt dies nicht, sodass sie nicht umgerüstet werden müssten.

205 Vgl. http://www.consilium.europa.eu/de/press/press-releases/2015/03/150302-emergency-call-system-road-accidents/.

206 Vgl. auch unter Kapitel 3, Teil 7, II.1..

207 Dieser enthält unter anderem Angaben zu Unfallzeitpunkt, Standort, Fahrtrichtung und Fahrzeug-Identifikationsnummer, vgl. https://de.wikipedia.org/wiki/ECall.

208 „*Global Navigation Satellite System*“.

209 Vgl. https://www.bmvi.de/SharedDocs/DE/Artikel/DG/ecall-fuer-mehr-sicherheit-im-strassenverkehr.html?linkToOverview=js.

210 Vgl. *Bach*, Auto Zeitung (20/2013), S. 88-89 (89).

211 Vgl. http://www.europarl.europa.eu/news/de/news-room/content/20120703IPR48185/html/Lebensrettendes-eCall-Notrufsystem-soll-in-alle-neuen-Autos-eingebaut-werden.

welche Auswirkungen der Einbau eines solchen Systems haben kann, insbesondere in Bezug auf Missbrauchsgefahren. Allerdings müssen die Aspekte der Verkehrssicherheit und die dadurch implizierte Reduzierung von Verkehrstoten dem entgegengehalten werden.

In technischer Hinsicht müssen Kraftfahrzeuge dazu unter anderem ausgestattet werden mit einem GPS-Empfänger zur Feststellung der Fahrzeugposition, einer GSM[212]-Antenne zum Senden des Notrufs an die Notrufzentrale, einem Steuergerät zur Standortmeldung über eine Mobilfunkeinheit, einem Crash-Sensor zum Erkennen aller Unfallarten, Mikrofon und Lautsprecher zur Kommunikation mit der Notrufzentrale und einer Taste zur manuellen Auslösung für den Fall einer plötzlichen Erkrankung.[213]

Heutzutage gibt es jedoch auch bereits herstellereigene Notrufsysteme, wie z.B. den *„Intelligenten Notruf"* von BMW. Bei diesem wird im Gegensatz zum eCall keine direkte Sprachverbindung mit der Notrufleitstelle hergestellt, sondern vielmehr eine solche zu einem BMW-Callcenter, was insoweit laut BMW als Filter wirken solle, als dass nur *„echte"* Notrufe die Rettungsleitstelle erreichen würden.[214]

Insgesamt stellen sowohl die herstellereigenen Systeme als auch das geplante eCall-System typische Big Data-Anwendungen dar. Durch den an die Notrufleitstelle übermittelten MSD kann dort durch Auswertung und Analyse der Daten bereits festgestellt werden, welche Verletzungen vorliegen, wie viele Personen beteiligt sind und daraus resultierend wie viele Rettungswagen benötigt werden. Aus der Verknüpfung der einzelnen Daten lässt sich somit das Szenario vor Ort analysieren. Durch die Einführung des eCalls kann also auf lange Sicht die Verkehrssicherheit wesentlich erhöht werden.

Es bleibt aber auch abzuwarten, wie möglichen Fehlfunktionen entgegengetreten werden soll, wenn z.B. bei einem Unfall mit zwei Kraftfahrzeugen bei beiden der eCall ausgelöst wird und letztlich zu viele Rettungswagen zum Unfallort geschickt würden. Insgesamt werden jedenfalls bei der Übertragung des MSD und durch die aufgebaute Sprechverbindung persönliche Daten bekannt und gespeichert. Insoweit ist auch hier die datenschutzrechtliche Relevanz offensichtlich.

---

212 „*Global System for Mobile Communication*".

213 Vgl. http://www.adac.de/infotestrat/unfall-schaeden-und-panne/ecall_gps_notruf/.

214 Vgl. http://www.bmvi.de/SharedDocs/DE/Anlage/VerkehrUndMobilitaet/Strasse/ivs-bmw-intelligenter-notruf.pdf?__blob=publicationFile.

Teil 6: Ausblick: Autonomes Fahren in der Zukunft

Der Wunsch nach autonomem Fahren ist keine Vision der Gegenwart und Zukunft. Die Idee vom selbstfahrenden Auto reicht bis in die Mitte des letzten Jahrhunderts zurück. Bereits im Jahr 1955 entwickelten Forscher des ehemaligen US-Elektronikkonzerns RCA in Zusammenarbeit mit dem Staat Nebraska und General Motors die sog. elektronische Autobahn, bei der ein System aus Kabeln und Transistoren in die Fahrbahn integriert werden und Autos selbständig vorwärts rollen sollten.[215] Es blieb jedoch bei einer Idee. Eine Umsetzung und Entwicklung erfolgt nicht.

Aber auch heute noch schreitet die Entwicklung in der Automobilbranche derart zügig voran, dass ein autonomes Fahren technisch gesehen in einigen Jahren tatsächlich greifbar sein kann. Studien zufolge könnte die Zahl autonomer Kraftfahrzeuge bis zum Jahr 2035 auf weltweit 95 Millionen ansteigen.[216]

Allerdings sind insoweit auch die rechtlichen Grundlagen zu beachten, die derzeit ein autonomes Fahren über lange Strecken und ohne jegliche Kontrolle oder Eingriffsmöglichkeit des Fahrers verhindern. Autopiloten stehen bei verschiedenen Herstellern zwar kurz vor der Serienreife, können aber derzeit lediglich auf Testgeländen erprobt werden.[217] Obwohl die bestehende Rechtsordnung vom Leitbild eines im Kraftfahrzeug anwesenden Fahrers ausgeht, ist die Idee des vollautonomen Fahrens durch die stetig fortschreitende Entwicklung im Bereich der Fahrerassistenzsysteme in den Fokus der Aufmerksamkeit gerückt.[218]

Es werden dabei vier Arten autonomen Fahrens[219] unterschieden, die nach und nach[220] Realität werden könnten. Das beweist auch das selbstfahrende Kraftfahrzeug von

---

215 Vgl. ADAC Motorwelt (3/2015), S. 10.

216 Vgl. http://www.handelsblatt.com/auto/test-technik/google-baut-eigenes-selbstfahrendes-auto-sieht-so-die-zukunft-des-autos-aus-seite-all/9961054-all.html.

217 Vgl. http://www.focus.de/auto/autoentwicklung/technik/auto-und-technik-autopilot-an-bord_id_3635914.html.

218 Vgl. *Lutz/Tang/Lienkamp*, NZV 2013, S. 57-63 (57).

219 Sog. assistiertes Fahren gibt es heute schon in Form von ESP und Abstandsregeltempomat. Sog. teilautomatisiertes Fahren verlangt vom Fahrer die Überwachung der Fahraufgabe, wie z.B. beim Stauassistenten, während sich das Kraftfahrzeug beim sog. hochautomatisierten Fahren schon in vielen Situationen selbst steuert, der Fahrer aber jederzeit eingreifen kann. Zuletzt gibt es noch das sog. vollautomatisierte Fahren, bei welchem der Fahrer auf der Rückbank platznehmen könnte, vgl. *Bloch*, Auto Motor und Sport (4/2014), S. 62-69 (64, 66).

Google, das in den USA als *„Google Self-Driving Car“* mittlerweile eine Strecke von fast 2,7 Millionen Kilometer unfallfrei zurückgelegt hat.[221] Insgesamt sind heutzutage schon Systeme am Markt, die das assistierte und das teilautomatisierte Fahren ermöglichen.[222] Dabei geht es insbesondere darum, Verlässlichkeit in Situationen zu schaffen, für die der Mensch am Steuer zur Fehlerquelle werden kann und dem Fahrer den belastenden Teil des Autofahrens abzunehmen, nämlich gleichförmige, sich immer wiederholende Abläufe wie z.B. den Stop-and-Go-Verkehr auf der Autobahn.[223]

Es zeigt sich ein Wandel der eigentlichen Fahraufgabe von einem aktiven Steuern (Lenken, Beschleunigen, Bremsen usw.) hin zu einer bloßen Überwachung der Fahrzeugbewegungen.[224] Der Weg der Entwicklungen führt hin zur sog. *„Vision Zero“*, nach welcher es zukünftig keine Verkehrstoten, keine Schwerverletzten und schließlich auch keine Unfälle mehr geben soll.[225] Dass dies auch bei autonomem Fahren nicht gänzlich umsetzbar ist, zeigt der erste tödliche Unfall bei Fahren mit eingeschaltetem Autopiloten.[226] Zentrale Entwicklungsschwerpunkte sind deshalb weiterhin ein Sensorkonzept für die 360°-Umfelderfassung, eine Funktionssicherheit gegen Fehlfunktionen und Angriffe von außen, hochgenaue Kartendaten mit einer Auflösung bis zu 10 Zentimetern sowie letztlich die rechtlichen Regelungen.[227]

Denn bislang ist es rechtlich nicht möglich, Fahrertätigkeiten vollständig aus den Händen zu geben. Grund dafür sind die Regelungen des *„Wiener Übereinkommens über den Straßenverkehr vom 08. November 1968“* (WÜ-StV).[228] Obwohl das Wiener Überein-

---

220 Die Continental Aktiengesellschaft geht davon aus, dass teilautomatisiertes Fahren im Jahr 2016, hochautomatisiertes Fahren im Jahr 2020 und vollautomatisiertes Fahren ab dem Jahr 2025 in der Automobilindustrie umsetzbar sein sollen, vgl. http://www.continental-corporation.com/www/presseportal_com_de/allgemein/automatisiertes-fahren/automatisiertes-fahren-intro-de.html.

221 Vgl. http://www.sueddeutsche.de/auto/testphase-des-google-car-mensch-gegen-maschine-1.2632147.

222 Vgl. VDA Jahresbericht 2014, https://www.vda.de/de/services/Publikationen/jahresbericht-2014.html.

223 Vgl. *Jourdan/Matschi*, NZV 2015, S. 26–29 (27).

224 Vgl. *Jänich/Schrader/Reck*, NZV 2015, S. 313-318 (313).

225 Vgl. *Jourdan/Matschi,* NZV 2015, S. 26–29 (26).

226 Vgl. http://www.heise.de/newsticker/meldung/Toedlicher-Unfall-mit-Teslas-Autopilot-3252120.html.

227 Vgl. http://www.springerprofessional.de/automatisiertes-fahren-was-noch-getan-werden-muss/5018728.html.

228 Vgl. dazu unter *Kapitel 2, Teil 3, I.*.

kommen über den Straßenverkehr nach Art. 1 Abs. 2 des Ratifikationsgesetzes[229] keine unmittelbare Anwendung in Deutschland findet, muss die Bundesrepublik nach Art. 3 Abs. 1 lit. a Satz 1 WÜ-StV sicherstellen, dass die nationalen Verkehrsregeln den Vorgaben des Wiener Übereinkommens entsprechen.[230] Danach ist völkerrechtlich geregelt, dass ein Fahrer immer und in jeder Situation die Kontrolle über sein Kraftfahrzeug haben muss.[231] In Art. 8 Abs. 5 WÜ-StV heißt es:

> *„Jedes Fahrzeug und miteinander verbundene Fahrzeuge müssen, wenn sie in Bewegung sind, einen Führer haben. (...) Jeder Führer muss dauernd sein Fahrzeug beherrschen (...) können.“.*

Die vom Fahrer nicht übersteuerbare Übertragung einer spezifischen Fahrbewegung auf ein Fahrerassistenzsystem ist demnach damit nicht vereinbar.[232] Damit in Zukunft ein autonomes Fahren auch rechtlich möglich ist, müssten insoweit die gesetzlichen Bestimmungen einer umfänglichen Änderung unterzogen werden.

Ein erster Schritt in diese Richtung konnte zwischenzeitlich durch die am 23.09.2014 verabschiedete und nach den Regularien des Übereinkommens[233] 18 Monate später und somit am 23.03.2016 in Kraft tretende Änderung des Art. 8 WÜ-StV erreicht werden.[234] Der dabei neu eingefügte Art. 8 Abs. 5bis lautet wie folgt:

> *„5bis. Fahrzeugsysteme, die einen Einfluss auf das Führen des Fahrzeugs haben, gelten mit Absatz 5 dieses Artikels und mit Absatz 1 des Artikels 13 als konform, sofern sie den Vorschriften bezüglich Bauweise, Montage und Benutzung nach Maßgabe der internationalen Rechtsvorschriften für Kraftfahrzeuge, Ausrüstungsgegenstände und Teile, die in Kraftfahrzeuge eingebaut und/oder dafür verwendet werden können, entsprechen;*
>
> *Fahrzeugsysteme, die einen Einfluss auf das Führen eines Fahrzeugs haben und die nicht den oben erwähnten Vorschriften bezüglich Bauweise, Montage und*

---

229 *Gesetz zu den Übereinkommen vom 8. November 1968 über den Straßenverkehr und über Straßenverkehrszeichen, zu den Europäischen Zusatzübereinkommen vom 1. Mai 1971 zu diesen Übereinkommen sowie zum Protokoll vom 1. März 1973 über Straßenmarkierungen vom 21.09.1977*, BGBl. II 1977, Nr. 39 vom 11.10.1977, S. 809.

230 Vgl. *Lutz*: Anforderungen an Fahrerassistenzsysteme nach dem Wiener Übereinkommen über den Straßenverkehr, in: NZV 2014, S. 67–72 (67).

231 Vgl. *Müller*, VW 2013, S. 10 sowie *Lutz/Tang/Lienkamp*, NZV 2013, S. 57-63 (58).; a.A. vgl. nur *Bewersdorf*, NZV 2003, S. 266-271 (271). Der Streitstand soll für die weitere Bearbeitung nicht maßgeblich sein.

232 Vgl. *Albrecht*, SVR 2005, S. 373-376 (373).

233 Vgl. Art. 49 Abs. 2 lit. a. Satz 3 WÜ-StV.

234 Vgl. https://www.auto-medienportal.net/artikel/detail/35082.

Benutzung entsprechen, gelten mit Absatz 5 dieses Artikels und mit Absatz 1 des Artikels 13 als konform, sofern die Fahrzeugsysteme vom Fahrzeugführer übersteuert oder deaktiviert werden können.“[235]

Danach sind nun erstmals Systeme erlaubt, die die Steuerung des Fahrzeugs beeinflussen können, aber jederzeit durch den Fahrer übersteuert oder gestoppt werden können müssen.[236] Die Systeme müssen dabei entweder den einschlägigen technischen Regelwerken der Vereinten Nationen entsprechen oder aber derart ausgestaltet sein, dass sie jederzeit vom Fahrer übersteuert oder abgeschaltet werden können.

Mit der vorgenannten Änderung ist zwar ein wesentlicher Schritt in Richtung autonomes Fahren und die dazu nötige rechtliche Anpassung der Regelwerke getan. Jedoch sind hier noch weitere, auch auf dieser Änderung basierende, Veränderungen und Anpassungen nötig. So ist es beispielsweise unumgänglich auch die sog. UN/ECE-Regelungen und dort insbesondere die UN/ECE-Regelung 79, anzupassen. Dieser von der Wirtschaftskommission für Europa mit den Vereinten Nationen vereinbarte Katalog einheitlicher Vorschriften für technische Einrichtungen bei Kraftfahrzeugen regelt derzeit noch, dass sich die Hände des Fahrers stets in Reichweite zum Lenkrad befinden müssen.[237] Auf internationaler Ebene sind bereits weitere Änderungen geplant. So soll die Begriffsbestimmung des *„Fahrers“* so erweitert werden, dass ihm künftig automatisierte Systeme mit voller Kontrolle über ein Fahrzeug gleichgestellt werden.[238] Aber auch ohne weitere Änderungen dürften Fahrzeuge jeglichen Automatisierungsgrades derzeit mit dem Übereinkommen vereinbar sein, wenn sie gemäß Art. 8 Abs. 5^{bis} S. 1 WÜ-StV den Anforderungen der UN/ECE-Regeln entsprechen, wobei weiterhin gänzlich führerlose Robotertaxis mangels in jedem Fall nach Art. 8 Abs. 1 WÜ-StV erforderlichem menschlichem Fahrer ausgeschlossen sein dürften.[239]

---

235 Vgl. zum bislang nur in englischer Sprache vorliegenden Originaltext die Übersetzung der Schweizerischen Bundeskanzlei, https://www.admin.ch/opc/de/official-compilation/2016/1019.pdf. Die amtliche englische Fassung ist zu finden unter ECE/TRANS/WP.1/145, S. 10, http://www.unece.org/fileadmin/DAM/trans/doc/2014/wp1/ECE-TRANS-WP1-145e.pdf.

236 So *Jarzombek*, Vorsitzender der Arbeitsgruppe Digitale Agenda der CDU/CSU-Bundestagsfraktion, vgl. FD-StrVR 2016, 376984.

237 Vgl. https://www.auto-medienportal.net/artikel/detail/35082.

238 So *Jarzombek*, FD-StrVR 2016, 377719.

239 Vgl. *Lutz,* DAR 2016, S. 55-56 (56).

Kapitel 3: Die rechtliche Zulässigkeit des Umgangs mit Beschäftigtendaten aus intelligenten Kraftfahrzeugen

Nunmehr soll unter Berücksichtigung der bestehenden technischen Möglichkeiten, Daten zu generieren, näher untersucht werden, wie mit solchen Daten im datenschutzrechtlichen Sinne umzugehen ist. Das Augenmerk soll sich schwerpunktmäßig auf den Umgang mit den Daten durch Arbeitgeber beziehen und insoweit Szenarien abbilden, die in Bezug auf Firmenfahrzeuge mit fortschreitender technischer Entwicklung bereits bestehen oder aber zu erwarten sind. Im Hinblick auf das Beschäftigungsverhältnis begründet sich dabei die besondere Schutzbedürftigkeit des Einzelnen durch das Abhängigkeitsverhältnis und durch die Ausübung von wirtschaftlicher und sozialer *„Macht"* gegenüber dem einzelnen Arbeitnehmer.[240]

Teil 1: Die historische Entwicklung des Datenschutzes

Einleitend soll hier ein Überblick über die historische Entwicklung des Datenschutzes gegeben werden. Dieser bezieht sich insbesondere auf die Entwicklungen im Beschäftigtendatenschutz.

I. Das erste Datenschutzgesetz der Welt

Das Datenschutzrecht in Deutschland fand seinen ersten Niederschlag in der Verabschiedung des 1. Hessischen Datenschutzgesetzes vom 30. September 1970. Bereits vier Jahre später verabschiedete auch Rheinland-Pfalz ein Gesetz gegen missbräuchliche Datennutzung (Gesetz v. 02.01.1974, GVBl. I 31).[241] Das erste Datenschutzgesetz auf Bundesebene wurde am 01.02.1977 im Bundesgesetzblatt verkündet[242] und trat in vollem Umfang am 01.01.1979 in Kraft. Diese Zeit war geprägt von der aktiven Vorgehensweise der Gesetzgebungsorgane, die ihr Tätigwerden mit der stetigen Automatisie-

240 So *Gola*: Betrieblicher Datenschutz, 1990, S. 21.

241 Im weiteren Verlauf schlossen sich auch Bremen (Gesetz v. 19.12.1977, BremGBl. 393), Bayern (Gesetz v. 28.04.1978, BayRS 204-1-I), das Saarland (Gesetz v. 17.05.1978, ABl. 581), Niedersachsen (Gesetz v. 26.05.1978, GVBl. 421), Schleswig-Holstein (Gesetz v. 01.06.1978, GVBl. 156) und Nordrhein-Westfalen (Gesetz v. 19.12.1978, GVNW. 640) an, vgl. *Ronellenfitsch* in Wolff/Brink: Datenschutzrecht in Bund und Ländern, 2013, Einleitung, Rn. 6.

242 *Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz - BDSG) vom 27.01.1977*, BGBl. I 1977, Nr. 7 vom 01.02.1977, S. 201.

rung der Datenverarbeitung sowie damit begründeten, dass sie sich mit Problemen auseinandersetzen würden, die sich innerhalb aller Verarbeitungsvorgänge stellten und deshalb in einem einheitlichen Gesetz zu regeln seien.[243] Diese Datenschutzgesetze erster Generation setzten den Fokus noch weitgehend auf die Verhinderung des Missbrauchs der Daten.[244] Das Bundesdatenschutzgesetz vom 27.01.1977 enthielt keine spezifisch Vorschriften zur Datenverwendung im Arbeitsverhältnis. Vielmehr gab es lediglich einzelne Verweisungen, wie z.B. in § 7 Abs. 3 BDSG 1977.[245]

II. Das Volkszählungsurteil des Bundesverfassungsgerichts

Schließlich folgte sodann im Jahr 1983 eine wegweisende gerichtliche Entscheidung für den Bereich des Datenschutzes. Das Bundesverfassungsgericht verkündete am 15.12.1983 sein Urteil zum Volkszählungsgesetz 1983[246], das sog. *„Volkszählungsurteil“*.[247] *Hoffmann-Riem* bezeichnete die Entscheidung rückblickend als *„Magna Charta der Entwicklung des deutschen Datenschutzrechts“*.[248] Der Symbolwert der Entscheidung ergab sich daraus, dass mit der Volkszählung für die Menschen ein kollektives Erlebnis zustande kam, indem sich jeder Bürger zum gleichen Zeitpunkt mit den gleichen Informationsanforderungen konfrontiert sah.[249] Die Voraussetzungen zur Verarbeitung personenbezogener Daten wurden insoweit durch das Volkszählungsurteil neu geformt, dass der Verarbeitungsradius durch die Forderung nach einer klaren Zweckbindung im Voraus einzuschränken war.[250] In dem Urteil wurde aus Art. 1 Abs. 1 iVm Art. 2 Abs. 1 GG das verfassungsrechtlich gewährleistete Recht auf informationelle Selbstbestimmung hergeleitet:

---

243 Andere Aspekte für das Tätigwerden der Gesetzgebungsorgane waren der Informationsvorsprung der Regierung korrespondierend mit der tendenziellen Degradierung der Betroffenen zu beliebig steuerbaren Objekten, vgl. *Simitis* in Simitis: Bundesdatenschutzgesetz, [8]2014, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 6, 18, 21.

244 Erst nach der Novellierung des Bundesdatenschutzgesetzes im Jahr 1990 zielte das Bundesdatenschutzgesetz auf den Schutz des Einzelnen vor einem Umgang mit personenbezogenen Daten, der sein Persönlichkeitsrecht beeinträchtigt, vgl. *Roßnagel* in Roßnagel: Handbuch Datenschutzrecht, 2003, 1. Einleitung, Rn. 19, 22.

245 Vgl. *Gola/Wronka*: Handbuch zum Arbeitnehmerdatenschutz, 1989, S. 20

246 *Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz 1983) vom 25.03.1982*, BGBl. I 1982, Nr. 13 vom 31.03.1982, S. 369.

247 Bundesverfassungsgericht, Urteil vom 15.12.1983, Aktenzeichen 1 BvR 209/83, NJW 1984, S. 419-428.

248 Vgl. *Hoffmann-Riem*, AöR 123 (1998), S. 513-540 (515).

249 Vgl. *Simitis* in Simitis: Bundesdatenschutzgesetz, [8]2014, Einführung: Geschichte – Ziele – Prinzipien, Rn. 28.

250 Vgl. *Simitis* in Simitis: Bundesdatenschutzgesetz, [8]2014, Einführung: Geschichte – Ziele – Prinzipien, Rn. 38.

„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine dies ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. (...) Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe der persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."[251]

Eine weitere besondere Ausprägung des Allgemeinen Persönlichkeitsrechts nach Art. 1 Abs. 1 iVm Art. 2 Abs. 1 GG kristallisierte sich in der Entscheidung des Bundesverfassungsgerichts vom 27.02.2008[252] in Form des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme heraus. Dieses Grundrecht gewährleistet den Schutz vor Eingriffen in informationstechnische Systeme, soweit nicht bereits ein Schutz insbesondere durch Art. 10 GG oder Art. 13 GG sowie das Recht auf informationelle Selbstbestimmung gewährleistet ist.[253]

III. Die Novelle des Bundesdatenschutzgesetzes im Jahr 2009

Die im Jahr 2009 erfolgte zweite Novelle des Bundesdatenschutzgesetzes (BDSG-Novelle II) wurde maßgeblich durch Datenschutzskandale angeregt, bei denen es insbesondere zu illegalem Datenhandel sowie ausufernden Mitarbeiterkontrollen kam.[254] Das Bundesdatenschutzgesetz erfuhr dadurch in Einzelbereichen eine weitere Modernisierung, die gleichzeitig auch die nach derzeitigem Stand letzte Änderung des Bundesda-

---

251 Bundesverfassungsgericht, Urteil vom 15.12.1983, Aktenzeichen 1 BvR 209/83, NJW 1984, S. 419-428 (422)

252 Bundesverfassungsgericht, Urteil vom 27.02.2008, Aktenzeichen 1 BvR 370/07, 1 BvR 595/07, NJW 2008, S. 822-837.

253 Vgl. *Ronellenfitsch* in Wolff/Brink: Datenschutzrecht in Bund und Ländern, 2013, Einleitung, Rn. 7.

254 Vgl. *Gola/Schomerus*: BDSG, [12]2015, Einleitung, Rn. 24.

tenschutzgesetzes durch Art. 1 des Gesetzes zur Änderung datenschutzrechtlicher Vorschriften vom 14.08.2009 darstellt.[255]

Die BDSG-Novelle II im Jahr 2009 setzte ein erstes Zeichen auf dem Weg zu einer bereichsspezifischen Regelung zum Beschäftigendatenschutz in Gestalt des neu eingefügten § 32 BDSG 2009. Zwar wurde gleichzeitig in § 3 Abs. 11 BDSG 2009 eine Legaldefinition des Beschäftigtenbegriffs eingeführt, darin erschöpften sich allerdings die bereichsspezifischen Regelungen zum Beschäftigtendatenschutz. Noch dazu wurde festgelegt, dass durch die Einführung des § 32 BDSG 2009 ein Arbeitnehmerdatenschutzgesetz weder entbehrlich sein noch inhaltlich präjudiziert werden solle.[256] Es stand somit schon zu diesem Zeitpunkt fest, dass die Vorschrift des § 32 BDSG 2009 nur als vorübergehende Regelung zu verstehen sein sollte. Somit brachte die BDSG-Novelle II 2009 zwar eine bereichsspezifische Regelung zum Beschäftigtendatenschutz, die aber zugleich nur als Übergangsregelung fungieren und deshalb nicht als hinreichende Grundlage dienen sollte.

IV. Der Versuch einer Novelle des Beschäftigtendatenschutzes

In der der BDSG-Novelle II 2009 folgenden Legislaturperiode wurde das Bestreben nach einem eigenen Beschäftigtendatenschutzgesetz erneut verfolgt. Dazu legte die SPD-Fraktion im Bundestag einen Entwurf eines Gesetzes zum Datenschutz im Beschäftigtenverhältnis vor.[257] Bereits knapp vier Monate später legte das Bundesinnenministerium ein Eckpunktepapier zu den Grundüberlegungen zur Ausarbeitung eines Gesetzesentwurfs vor[258], um sodann zum 28.05.2010 einen Referentenentwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes zu erarbeiten[259]. Nach diesem sollte durch die klaren gesetzlichen Regelungen die Rechtssicherheit im Beschäftigungsverhältnis erhöht werden. Dies fand Ausdruck in 14 die allgemeine Zulässigkeitsnorm des § 32 BDSG ergänzenden Vorschriften.

---

255 *Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 14.08.2009*, BGBl. I 2009, Nr. 54 vom 14.08.2009, S. 2814.

256 BT-Drs. 16/13657 vom 01.07.2009, S. 20, http://dipbt.bundestag.de/dip21/btd/16/136/1613657.pdf.

257 BT-Drs. 17/69 vom 25.11.2009, http://dip21.bundestag.de/dip21/btd/17/000/1700069.pdf.

258 Darin wird nochmals festgehalten, dass sich die Regierungsparteien darüber einig seien, dem Beschäftigtendatenschutz ein eigenes Kapitel im Bundesdatenschutzgesetz zu widmen, vgl. www.bmi.bund.de/cae/servlet/contentblob/941830/publicationFile/60604/eckpunkte_an_datenschutz.pdf.

259 Vgl. https://www.iitr.de/images/stories/referentenentwurf_beschaeftigtendatenschutz.pdf.

Nachdem verschiedenste Gruppierungen zu diesem Entwurf Stellung genommen hatten[260], beschloss die Bundesregierung den Entwurf am 25.08.2010.[261] In einem Hintergrundpapier[262] wurde erläutert, dass der Gesetzesentwurf insbesondere Regelungen zur offenen Videoüberwachung von nicht öffentlich zugänglichen Betriebsstätten, dem Einsatz von Ortungssystemen und der Datenverarbeitung zum Zweck der Leistungs- und Verhaltenskontrolle treffen sollte. Zudem würden strenge Voraussetzungen an die Datenverarbeitung ohne Kenntnis des Beschäftigten gestellt. Trotz erheblicher Kritik seitens des Bundesrates[263] leitete die Bundesregierung den Gesetzesentwurf ohne wesentliche Änderungen dem Bundestag zu.[264] Am 25.02.2011 erfolgte in erster Lesung im Bundestag eine Beratung des von der Bundesregierung eingebrachten Gesetzesentwurfes unter Weiterverweisung in die zuständigen Ausschüsse.[265]

Auch die Justizministerkonferenz beschäftigte sich im Laufe des Jahres 2011 mit dem Arbeitnehmerdatenschutz. Bereits auf deren Frühjahrskonferenz in Halle (Saale) im Mai 2011 stellte sie fest, dass der Gesetzesentwurf noch änderungs- und ergänzungsbedürftig sei, insbesondere sei ein hohes Maß an Transparenz anzustreben, indem Arbeitgeber zu verpflichten seien, ihre Arbeitnehmer darüber zu unterrichten, welche Daten intern wie auch extern über sie erhoben und gespeichert würden.[266] Im Rahmen der Herbstkonferenz im November 2011 in Berlin bekräftigten die Justizminister ihren Standpunkt, es bestünde erheblicher Änderungs- und Ergänzungsbedarf hinsichtlich des Gesetzesentwurfes, und verwiesen insoweit auf die Ergebnisse der öffentlichen Anhörung im Innenausschuss des Bundestages.[267] Eine umfassende Regelung des Beschäftigtendatenschutzes sei unbedingt erforderlich.

---

260 Zu dem Referentenentwurf haben u.a. Stellung genommen der Deutsche Gewerkschaftsbund (pdf-Datei, hinterlegt beim DGB), der Deutsche Richterbund (http://www.drb.de/cms/index.php?id=655) und der Deutsche Anwaltverein durch den Arbeitsrechtsausschuss (pdf-Datei, hinterlegt beim DAV).

261 Vgl. den Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes, Bearbeitungsstand: 24.08.2010, http://www.cr-online.de/ArbDS-RegE.pdf..

262 Vgl. pdf-Datei, hinterlegt beim BMI.

263 BR-Drs. 535/2/10 vom 25.10.2010, http://dipbt.bundestag.de/dip21/brd/2010/0535-2-10.pdf sowie BR-Drs. 535/10(B) vom 05.11.2010, http://dipbt.bundestag.de/dip21/brd/2010/0535-10B.pdf.

264 BT-Drs. 17/4230 vom 15.12.2010, http://dipbt.bundestag.de/dip21/btd/17/042/1704230.pdf.

265 BT-Plenarprotokoll 17/94 vom 25.02.2011, S. 10745, http://dip21.bundestag.de/dip21/btp/17/17094.pdf.

266 Vgl. Beschluss der Frühjahrskonferenz der Justizministerinnen und Justizminister am 18. und 19. Mai in Halle (Saale), TOP I.10: Arbeitnehmerdatenschutz, https://www.justiz.nrw.de/JM/leitung/jumiko/beschluesse/2011/fruehjahrskonferenz11/index.php.

267 Vgl. Beschluss der Herbstkonferenz der Justizministerinnen und Justizminister am 9. November 2011 in Berlin, TOP I.5: Arbeitnehmerdatenschutz, https://www.justiz.nrw.de/JM/leitung/jumiko/beschluesse/2010/herbstkonferenz10/index.php

Nach dieser letzten Kritik an dem Gesetzesentwurf vergingen mehr als zehn Monate, bis sich die Bundesregierung erneut aufgrund einer Kleinen Anfrage der Fraktion Die Linke[268] zu dem Gesetzesentwurf und der weiteren Planung zur Stellungnahme veranlasst sah. In ihrer Antwort erklärte die Bundesregierung, es habe insgesamt zustimmende und ablehnende Stimmen zum Gesetzesentwurf gegeben, sie halte diesen jedoch in der vorgelegten Fassung weiterhin für *„ausgewogen und in der Sache richtig“*.[269] Die Bundesregierung verteidigte den Gesetzesentwurf also weiterhin trotz nicht nachlassender Kritik.

Diese kam auch am 14.01.2013 von Seiten des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Peter Schaar. Bereits der Gesetzesentwurf an sich enthalte viele Schwachstellen, die durch die vorgeschlagenen Änderungen nur noch weiter verschlechtert würden.[270] Er betonte, dass es ein schlechtes Signal darstelle, wenn der Gesetzesentwurf teilweise hinter der von der Europäischen Kommission vorgeschlagenen Datenschutz-Grundverordnung (DS-GVO)[271] zurückbleibe. Nach diesem letzten Paukenschlag gegen den Gesetzesentwurf gab die Bundesregierung die Pläne für ein Beschäftigtendatenschutzgesetz wegen vielfältiger Widerstände bei Arbeitgebern und Gewerkschaften auf. Und erneut wurde die Suche nach einer Lösung auf die nächste Legislaturperiode verschoben. Die Schlagzeile

> *„Gestoppt! Bundesregierung zieht Notbremse beim Beschäftigtendatenschutz“*
> [272]

schlug Wellen in allen Bereichen und wurde überwiegend begrüßt.

Zuletzt stellte das Land Baden-Württemberg einen Antrag beim Bundesrat, über eine von ihm vorgelegte Entschließung zum Beschäftigtendatenschutz eine Sachentscheidung zu treffen.[273] Danach sollte der Bundesrat die Bundesregierung auffordern, in dem Verfahren auf Erlass einer Datenschutz-Grundverordnung der Europäischen Union darauf hinzuwirken, dass dabei die Voraussetzungen für ein künftiges Bundesgesetz und

---

268 BT-Drs. 17/10540 vom 22.08.2012, http://dip21.bundestag.de/dip21/btd/17/105/1710540.pdf.
269 BT-Drs. 17/10666 vom 12.09.2012, S. 4, http://dip21.bundestag.de/dip21/btd/17/106/1710666.pdf2.
270 Vgl. http://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2013/02_KeinGrosserWurf.html?nn=5217154.
271 Vgl. unter *Kapitel 3, Teil 1, V.*.
272 Vgl. http://www.haufe.de/personal/arbeitsrecht/beschaeftigtendatenschutz-gesetz-von-bundesregierung-gestoppt_76_167180.html.
273 BR-Drs. 552/13 vom 28.06.2013, http://dipbt.bundestag.de/doc/brd/2013/0552-13.pdf.

durch den nationalen Gesetzgeber effektive Grundlagen geschaffen würden. Die geforderte *„sofortige Sachentscheidung“* erfolgte nicht. Dies war vorerst der letzte Versuch der Schaffung eines Beschäftigtendatenschutzgesetzes.

Nach dem Erlass der Datenschutzgrundverordnung[274] besteht für den nationalen Gesetzgeber nun allerdings eine neue rechtliche Grundlage, um auch national weiter tätig zu werden. Das deutsche Recht muss an die Datenschutz-Grundverordnung angepasst und individuelle Regelungen zu den sogenannten Öffnungsklauseln gefunden werden.[275]

V. Datenschutz auf europäischer Ebene

Im Hinblick auf den sich rasant entwickelnden europäischen Binnenmarkt bedurfte es europaeinheitlicher Regelungen, die als völkerrechtliches Abkommen[276] generiert wurden, die wiederum seit Verabschiedung des Ratifikationsgesetzes[277] am 01.10.1985 geltendes Recht ist.[278]

Zur Vermeidung von Wettbewerbsverzerrungen sollte ein Ausgleich des Datenschutzniveaus der einzelnen Mitgliedsstaaten durch Erlass der sog. Datenschutz-Richtlinie (DS-RL)[279] herbeigeführt werden.[280] Obwohl Bundesgesetzgeber wie auch Landesgesetzgeber verpflichtet waren, das Datenschutzrecht der Richtlinie innerhalb von drei Jahren, d.h. bis zum 24.10.1998 anzupassen, vergingen bis zum Inkrafttreten des Bundesdatenschutzgesetzes 2001[281] noch weitere zweieinhalb Jahre.[282] Der Bundesgesetzgeber setzte durch die Neufassung des Bundesdatenschutzgesetzes vom 18.05.2001[283] die Vorgaben der Datenschutz-Richtlinie um, insbesondere bezüglich des grundsätzli-

---

274 Vgl. unter *Kapitel 3, Teil 1, V.*.

275 Vgl. https://berliner-datenschutzrunde.de/node/208.

276 *Konvention des Europarates zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten vom 28.01.1981.*

277 *Gesetz zu dem Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten vom 13. März 1985*, BGBl. II 1985, Nr. 12 vom 19.03.1985, S. 538.

278 Vgl. *Gola*: Betrieblicher Datenschutz, 1990, S. 15

279 *Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr*, ABl. EG Nr. L 181, S. 31-50.

280 Vgl. *Roßnagel* in Roßnagel: Handbuch Datenschutzrecht, 2003, 1. Einleitung, Rn. 23.

281 *Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18. Mai 2001*, BGBl. I 2001, Nr. 23 vom 22.05.2001, S. 904.

282 Nur in Hessen und Brandenburg gelang die fristgerechte Umsetzung, vgl. *Gola/Schomerus*: BDSG, ^{12}2015, Einleitung Rn. 10 f..

283 *Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18. Mai 2001*, BGBl. I 2001, Nr. 23 vom 22.05.2001, S. 904.

chen Verbots der Verarbeitung besonderer Daten (z.B. Gesundheitsdaten), des Verbots automatisierter Einzelentscheidungen und Elementen der Selbstregulierung.[284]

1. Reform des europäischen Datenschutzrechts

Am 25.01.2010 schlug die Kommission eine umfassende Reform der Datenschutzvorschriften auf europäischer Ebene vor und veröffentlichte dazu eine Mitteilung zu einem *„Gesamtkonzept für den Datenschutz in der Europäischen Union"*.[285] Neben einer Mitteilung über die politischen Ziele der Kommission[286] umfassten die konkreten Vorschläge der Kommission auch zwei Legislaturvorschläge in Form der sog. Datenschutz-Grundverordnung[287] sowie einer Richtlinie[288] speziell zum Schutz personenbezogener Daten, die zum Zweck der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten und für damit verbundene justizielle Tätigkeiten verarbeitet werden.

Die Rechtsgrundlage dafür, dass die Europäische Union datenschutzrechtliche Vorschriften erlassen kann, findet sich in Art. 16 Abs. 2 AEUV.

2. Datenschutz-Grundverordnung

Besondere Bedeutung hat im vorliegenden Fall die sog. Datenschutz-Grundverordnung (DS-GVO). Diese soll als Ersatz für die Datenschutz-Richtlinie dienen.[289] Dabei ist zunächst zu beachten, dass es sich bei dieser – im Gegensatz zur bisherigen Datenschutz-Richtlinie – um eine Verordnung handelt. Die Änderung der Rechtsform ist hier deshalb von besonderer Wichtigkeit, da eine Verordnung keiner Umsetzung in den einzelnen

---

284 Vgl. *Tinnefeld/Buchner/Petri*: Einführung in das Datenschutzrecht, [5]2012, S. 69.

285 *Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Gesamtkonzept für den Datenschutz in der Europäischen Union*, KOM (2010) 609 endg., http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_de.pdf.

286 *Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Der Schutz der Privatsphäre in einer vernetzten Welt, Ein europäischer Datenschutzrahmen für das 21. Jahrhundert*, KOM (2012) 9 endg., http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_9_de.pdf.

287 *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) vom 25.01.2012*, KOM (2012) 11 endg., http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM%282012%290011_DE.pdf.

288 *Vorschlag für Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr vom 25.01.2012*, KOM (2012) 10 endg., http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:DE:PDF.

289 Vgl. *Tinnefeld/Buchner/Petri*: Einführung in das Datenschutzrecht, [5]2012, S. 124.

Mitgliedsstaaten mehr bedarf, sondern vielmehr unmittelbare Geltung beansprucht.[290] Insoweit generiert eine Verordnung für die Mitgliedsstaaten ein *„Umsetzungsverbot"* und stellt eine abschließende Regelung dar, sofern keine Öffnungsklausel enthalten ist.[291]

a) Gesetzgebungsverfahren

Der Bundestag hat zu dem Kommissionsvorschlag am 06.11.2012 Stellung genommen.[292] Bereits am 16.01.2013 legt der Berichterstatter Jan Philipp Albrecht dem Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments einen Berichtsentwurf vor, in dem Änderungsvorschläge hinsichtlich des Entwurfs der Datenschutz-Grundverordnung vorgestellt wurden.[293] Daraufhin einigte sich das Europäische Parlament auf einen Entwurf für eine Änderung der von der Kommission vorgelegten Datenschutz-Grundverordnung.[294] Auch hierzu legte der Berichterstatter Jan Philipp Albrecht dem Europäischen Parlament den Bericht des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres vor.[295] Sowohl am 05.12.2013 als auch am 04.03.2014 wurde der Entwurf der Datenschutz-Grundverordnung im Rat erörtert, was in beiden Fällen ohne Ergebnis blieb.

Doch bereits am 12.03.2014 fand über den Entwurf der Datenschutz-Grundverordnung in erster Lesung eine Beratung im Europäischen Parlament statt, in der im Rahmen einer Legislativen Entschließung der Position des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres zugestimmt wurde.[296] Das Europäische Parlament stimmte mit 621 gegen 10 Stimmen bei 22 Enthaltungen der Datenschutz-Grundverordnung zu.[297] Der Europäische Rat einigte sich am 06.06.2014 zumindest über einige Aspekte des Entwurfs der Datenschutz-Grundverordnung. Diese Allgemeine Ausrichtung erfasste

---

290 Vgl. Art. 288 Abs. 2 AEUV.
291 So *Eckhardt/Kramer/Mester*, DuD 2013, S. 623–630 (624).
292 BT-Drs. 17/11325 vom 06.11.2012, http://dipbt.bundestag.de/dip21/btd/17/113/1711325.pdf.
293 Vgl. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-501.927%2b04%2bDOC%2bPDF%2bV0%2f%2fDE.
294 Hinterlegt auf den Internetseiten des EP-Abgeordneten Weidenholzer, http://www.weidenholzer.eu/wp-content/uploads/2013/10/EUDATAP_allcompromises.pdf.
295 Vgl. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bREPORT%2bA7-2013-0402%2b0%2bDOC%2bPDF%2bV0%2f%2fDE.
296 Vgl. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//DE.
297 So *Philipp*, EuZW 2014, S. 283 (283).

jedoch bislang insbesondere nur die Vorschriften zur Übermittlung von Daten in Nicht-EU-Mitgliedsstaaten.[298]

Im weiteren Verlauf nahm der Rat der Europäischen Union am 10.10.2014 eine partielle allgemeine Ausrichtung zur Datenschutz-Grundverordnung an.[299] Diese partielle Ausrichtung bezog sich jedoch nur auf einen Teil der geplanten Datenschutz-Grundverordnung und betraf insoweit das Kapitel *„Für die Verarbeitung Verantwortlicher und Auftragsverarbeiter"*. Zuletzt erfolgte eine Einigung auf eine partielle allgemeine Ausrichtung auch hinsichtlich der Aufnahme des öffentlichen Sektors in den Anwendungsbereich des Entwurfs der Datenschutz-Grundverordnung sowie über spezifische Verarbeitungssituationen gemäß Kapitel IX.[300]

Unter dem 15.06.2015 haben sich die zuständigen Minister der Mitgliedsstaaten schließlich auf eine umfassende Allgemeine Ausrichtung zur Datenschutzgrundverordnung geeinigt.[301] Die Grundlage für die Trilogverhandlungen[302] zwischen Europäischem Parlament, Rat und Kommission war damit geschaffen. Dabei konnte am 15.12.2015 eine vorläufige Einigung, insbesondere hinsichtlich einer informierten Einwilligung als Eckpfeiler des Datenschutzkonzepts erzielt werden.[303] Am 28.01.2016 gab der Rat der Europäischen Union eine vorläufige deutsche Fassung der Datenschutz-Grundverordnung heraus.[304] Nachdem der Rat der Europäischen Union am 08.04.2016 die endgültige Fassung der Datenschutz-Grundverordnung gebilligt hatte[305], beschloss das Europäische Parlament die von der Europäischen Kommission vorgeschlagene Datenschutz-Grundverordnung am 14.04.2016[306].

---

298 Vgl. http://www.cep.eu/fileadmin/user_upload/CEP-Monitor/COM_2012_11_Datenschutz/cepMonitor_Datenschutz-GrundVO_Rat.pdf.

299 Vgl. http://data.consilium.europa.eu/doc/document/ST-13772-2014-INIT/de/pdf.

300 Vgl. http://register.consilium.europa.eu/doc/srv?l=de&f=ST%2016140%202014%20INIT.

301 Vgl. http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/de/pdf.

302 Die Möglichkeit informeller Trilogverhandlungen wurde durch die Gemeinsame Erklärung zu den praktischen Modalitäten des neuen Mitentscheidungsverfahrens (Art. 251 EGV) am 13.06.2007 festgelegt und darf in allen Phasen der Beschlussfassung nach Art. 294 AEUV genutzt werden, vgl. https://de.wikipedia.org/wiki/Trilog.

303 Vgl. https://www.datenschutz-mv.de/datenschutz/themen/grundvo/10_Punkte.pdf.

304 Vgl. http://www.cr-online.de/26378.htm.

305 Vgl. http://www.heise.de/newsticker/meldung/EU-Staaten-winken-umfangreiche-Datenschutzreform-durch-3166549.html.

306 Vgl. http://www.cr-online.de/26378.htm.

Die EU-Datenschutzgrundverordnung wurde sodann am 04.05.2016 im EU-Amtsblatt veröffentlicht und trat 20 Tage später in Kraft, sodass sie nach einer zweijährigen Übergangszeit am 25.05.2018 für Unternehmen und Behörden anwendbar sein wird.[307]

b) Rechtliche Inhalt der Datenschutz-Grundverordnung

Inhaltlich ist die nunmehr erlassene Datenschutz-Grundverordnung mit den im Gesetzgebungsverfahren vorgenommenen Änderungen eher kritisch zu beurteilen. Bereits in den Erwägungsgründen der Datenschutz-Grundverordnung wird festgestellt, dass die Ziele und Grundsätze der Datenschutz-Richtlinie[308] nach wie vor Gültigkeit besitzen sollen.[309] Während die gefestigte Rechtsprechung des Europäischen Gerichtshofs jedoch davon ausgeht, dass schon die Datenschutz-Richtlinie auf eine Vollharmonisierung des Datenschutzes ausgerichtet gewesen sei[310], vertritt die Kommission die Auffassung, die Datenschutz-Richtlinie habe eine unterschiedliche Handhabung des Datenschutzes nicht verhindern können[311] und tritt damit der Rechtsprechung des Europäischen Gerichtshofs entgegen. Die Kommission stellt vielmehr fest, dass der Zweck der Datenschutz-Grundverordnung darin liege, eine Harmonisierung der datenschutzrechtlichen Vorschriften zu erreichen.[312]

Allerdings soll dem nationalen Gesetzgeber auch weiterhin ein gewisser Gestaltungsspielraum verbleiben. Die gesetzliche Konkretisierung öffentlicher Aufgaben, für deren Zwecke eine Verarbeitung personenbezogener Daten vorgesehen sei, solle dem nationalen Gesetzgeber vorbehalten bleiben.[313] Gleichermaßen solle ihm die Gestaltung be-

---

307 Vgl. https://www.bvdnet.de/eu-dsgvo.html.

308 *Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, sog. Datenschutz-Richtlinie (DS-RL)*, ABl. EG Nr. L 181, S. 31-50.

309 Vgl. Erwägungsgrund (9) DS-GVO.

310 Europäischer Gerichtshof, Urteil vom 24.11.2011, Aktenzeichen C-468, 469/10, EuZW 2012, S. 37-40 (39). Allerdings sollte den Mitgliedsstaaten trotz alledem ein Gestaltungsspielraum verbleiben, vgl. Europäischer Gerichtshof, Urteil vom 06.11.2003, Aktenzeichen C-101/01, EuZW 2004, S. 245-252 (251) sowie Europäischer Gerichtshof, Urteil vom 29.01.2008, Aktenzeichen C-275/06, MMR 2008, S. 227-230 (229) und Europäischer Gerichtshof, Urteil vom 07.05.2009, Aktenzeichen C-553/07, EuZW 2009, S. 546-550 (548).

311 Vgl. Erwägungsgrund (9) DS-GVO.

312 Vgl. Erwägungsgrund (3) DS-GVO.

313 Vgl. *Tinnefeld/Buchner/Petri*: Einführung in das Datenschutzrecht, ^{5}2012, S. 126.

reichsspezifischer Regelungen[314] möglich bleiben.[315] Dies steht jedoch unter dem Vorbehalt entgegenstehender Rechtsakte, die die Kommission erlassen könnte. Denn die Kommission soll ermächtigt sein, in einer Vielzahl von Fällen delegierte Rechtsakte (sog. *delegated acts*)[316] sowie Durchführungsakte (sog. *implementing acts*)[317] zu erlassen, was wiederum im Ergebnis zu einer enormen Abstraktionshöhe der Datenschutz-Grundverordnung führt.[318]

Die Datenschutz-Grundverordnung sieht jedoch noch weitere Neuerungen bzw. Änderungen der bestehenden Regelungen und Handlungsweisen vor.

So wird ein Europäischer Datenausschuss geschaffen, für den die Mitgliedsstaaten mit mehreren Aufsichtsbehörden eine zentrale Kontaktstelle bestimmen.[319] Dadurch soll die durch die Datenschutz-Richtlinie eingesetzte Art. 29-Datenschutzgruppe als bisheriges unabhängiges Beratungsgremium ersetzt werden. Eine weitere beachtenswerte Neuerung ist die Einführung des sog. Prinzips des *„one stop shop"*, das nunmehr in Art. 55 Abs. 1 DS-GVO festgeschrieben ist. Danach soll für den Fall, dass ein für die Datenverarbeitung Verantwortlicher seine Niederlassungen in mehreren Mitgliedsstaaten hat, die Aufsichtsbehörde des Mitgliedsstaates zuständig sein, in dem sich die Hauptniederlassung befindet. Der Gefahr des sog. *„forum shopping"*[320] wird durch Einführung eines Kohärenzverfahrens begegnet werden, welches es den Aufsichtsbehörden erlaubt, die zuständige Aufsichtsbehörde bei dringendem Handlungsbedarf um eine Stellungnahme zu ersuchen, wenn die zuständige Aufsichtsbehörde trotz der Dringlichkeit keine Maßnahmen trifft.[321]

---

314 Dies gilt insbesondere für den Bereich des Beschäftigtendatenschutzes. Nach Art. 88 Abs. 1 DS-GVO können die Mitgliedsstaaten bei der Datenverarbeitung im Beschäftigungskontext für die dort genannten Zwecke – u.a. die Einstellung und die Erfüllung des Arbeitsvertrages – in den Grenzen der Verordnung die Verarbeitung personenbezogener Daten per Gesetz regeln. Durch diese Erfordernisse werden jedoch die mitgliedsstaatlichen Regelungsbefugnisse erheblich eingeschränkt, vgl. *Franzen*, DuD 2012, S. 322-326 (324).

315 Vgl. *Tinnefeld/Buchner/Petri*: Einführung in das Datenschutzrecht, [5]2012, S. 126.

316 Delegierte Rechtsakte sind Rechtsakte ohne Gesetzescharakter, mit denen die Kommission nicht wesentliche Vorschriften ergänzen und abändern kann, vgl. *Ruffert* in Calliess/Ruffert: EUV, AEUV Kommentar, [4]2011, Art. 290, Rn. 2.

317 Die Kommission ist danach dafür zuständig, entsprechende Durchführungsbestimmungen für die Durchführung von Gesetzgebungsakten zu erlassen, vgl. *Ruffert* in Calliess/Ruffert: EUV, AEUV Kommentar, [4]2011, Art. 291, Rn. 1.

318 Vgl. *Tinnefeld/Buchner/Petri*: Einführung in das Datenschutzrecht, [5]2012, S. 126.

319 Vgl. Art. 51 Abs. 3 DS-GVO.

320 Forum shopping meint die – zumeist unerwünschte – Möglichkeit, durch Auswahl eines von mehreren möglichen internationalen Gerichtsständen Einfluss auf das anzuwendende Sachrecht zu nehmen, vgl. Alpmann Brockhaus - Fachlexikon Recht, 2004, Stichwort "*Forum Shopping*", S. 517.

321 Vgl. Art. 63 DS-GVO.

Auch die Einwilligung in eine Datenverarbeitung wird in der Datenschutz-Grundverordnung an neue Voraussetzungen geknüpft. Insbesondere ist hervorzuheben, dass eine Einwilligung nicht möglich sein soll, wenn zwischen der Position des Betroffenen und der des für die Datenverarbeitung Verantwortlichen ein klares Ungleichgewicht bestehe.[322] Jeder Person steht zudem ein Recht auf Berichtigung der sie betreffenden personenbezogenen Daten zu sowie ein *„Recht auf Vergessenwerden"*[323], wenn die Speicherung ihrer Daten unter Verstoß gegen die Verordnung erfolgt ist. Zudem soll auf das Prinzip der Folgenabschätzung eingegangen werden. In Fällen der Datenverarbeitung, die aufgrund ihres Wesens, ihres Umfangs oder ihrer Zwecke konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen können, soll der für die Verarbeitung Verantwortliche vor der Verarbeitung eine Datenschutz-Folgenabschätzung (sog. data impact assessment) durchführen, die sich insbesondere mit den Maßnahmen befasst, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen dieser Verordnung nachgewiesen werden sollen.[324] Die Folgenabschätzung enthält zumindest eine allgemeine Beschreibung der vorgesehenen Verarbeitungsvorgänge und eine Bewertung der Risiken sowie der geplanten Abhilfemaßnahmen.[325]

Die Datenschutz-Grundverordnung umfasst auch bereits Regelungen zu technischen Entwicklungen, die insbesondere im vernetzten Fahrzeug eine entscheidende Rolle spielen. So findet sich in Art. 20 DS-GVO das sog. Recht auf Datenportabilität. Danach hat der Betroffene das Recht, von dem für die Verarbeitung Verantwortlichen eine Kopie der verarbeiteten Daten in einem von ihm weiter verwendbaren strukturierten, gängigen und maschinenlesbaren Format zu verlangen, wenn personenbezogene Daten elektronisch in einem strukturierten gängigen elektronischen Format verarbeitet werden. Dies könnte insoweit zur Datenvermeidung und Datensparsamkeit auf Seiten der verantwort-

---

322 Vgl. Erwägungsgrund (43) DS-GVO.

323 Dieser Aspekt war Gegenstand eines Urteils des Europäischen Gerichtshofs vom 13.05.2014 in der Rechtssache Google Spain / AEPD, Aktenzeichen C-131/12. Der Europäische Gerichtshof entschied, dass der Betreiber einer Internetsuchmaschine bei personenbezogenen Daten, die auf von Dritten veröffentlichten Internetseiten erscheinen, für die von ihm vorgenommene Verarbeitung verantwortlich ist. Eine Person könne sich daher, wenn bei einer anhand ihres Namens durchgeführten Suche in der Ergebnisliste ein Link zu einer Internetseite mit Informationen über sie angezeigt werde, unmittelbar an den Suchmaschinenbetreiber wenden, um unter bestimmten Voraussetzungen die Entfernung des Links aus der Ergebnisliste zu erwirken oder, wenn dieser ihrem Antrag nicht entspreche, an die zuständigen Stellen wenden, vgl. Europäischer Gerichtshof, Pressemitteilung Nr. 70/14, Urteil in der Rechtssache C-131/12, 13.05.2014, http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070de.pdf.

324 Vgl. Art. 35 Abs. 1 DS-GVO sowie Erwägungsgrund (84) DS-GVO.

325 Vgl. Art. 35 Abs. 7 DS-GVO.

lichen Stelle führen. Denn je weniger Daten des Betroffenen bei der verantwortlichen Stelle vorhanden sind, umso weniger Daten müsste sie gegebenenfalls für den Betroffenen portierbar machen.[326]

Insgesamt ist die Datenschutz-Grundverordnung also eher kritisch zu betrachten. Zunächst kann aufgrund der Abstraktionshöhe der Verordnung noch nicht klar gesagt werden, wie sich die Rechtslage unter Anwendung derselben darstellen wird. Vieles wird sich in dieser Hinsicht erst mit Erlass der ersten Durchführungsverordnungen und delegierten Rechtsakte zeigen. Insoweit besteht derzeit noch eine gewisse Unsicherheit. Diese wird dadurch verstärkt, dass die Datenschutz-Grundverordnung ihrer Rechtsnatur nach unmittelbare Wirkung in den Mitgliedsstaaten haben wird.[327] Insoweit besteht die Gefahr, dass die nationalen Grundrechte unterlaufen werden. Dies könnte also zu einem weitgehenden Verlust der Kontrolle an nationalen Grundrechten führen, insbesondere aufgrund der Tatsache, dass Art. 8 EU-GRCH kein materielles Schutzinstitut bietet, sondern vielmehr nur ein Recht auf Schutz der Daten.[328]

Kritisch zu hinterfragen sind außerdem die gewichtigen vorgenannten Befugnisse der Kommission, durch welche gleichzeitig die Befugnisse und Zuständigkeiten der einzelnen Mitgliedsstaaten reduziert und auf EU-Ebene verlagert werden. Dies droht zu einem Ungleichgewicht zwischen Mitgliedsstaaten auf der einen und Union auf der anderen Seite zu führen. Es bleibt abzuwarten, was sich aus der Anwendung der Datenschutz-Grundverordnung auf nationaler Ebene entwickeln wird.

VI. Einführung intelligenter Verkehrssysteme

Im Zusammenhang mit der sich rasant weiterentwickelnden Technik intelligenter Kraftfahrzeuge wurde mittlerweile die sog. IVS-RL[329] erlassen. Mit der IVS-RL wird im Interesse einer effizienteren, umweltverträglicheren und sichereren Mobilität das Ziel der Gewährleistung einer koordinierten und effektiven Einführung Intelligenter Verkehrssysteme im Straßenverkehr verfolgt.[330] In Umsetzung der IVS-RL legte die Bundesregierung dem Bundestag am 19.02.2013 einen Gesetzesentwurf für das sog. *Intelligente*

---

326 Vgl. *Conrad/Hausen* in Forgó: Betrieblicher Datenschutz, 2014, S. 217.
327 Vgl. Art. 288 Abs. 2 AEUV.
328 Vgl. *Schneider/Forgó/Helfrich* in Forgó: Betrieblicher Datenschutz, 2014, S. 27.
329 *Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern*, ABl. Nr. L 207 vom 06.08.2010, S. 1.
330 Vgl. ZD-Aktuell 2013, 03567.

Verkehrssysteme Gesetz (IVSG) vor.[331] Auf Empfehlung des Verkehrsausschusses[332] und aufgrund der Beschlussempfehlung wurde der Gesetzesentwurf sodann seitens des Bundestages am 21.03.2013 angenommen. Der Bundesrat billigte den Gesetzesentwurf am 03.05.2013.[333] Das Intelligente Verkehrssysteme Gesetz trat schließlich am 21.06.2013 in Kraft.[334]

Die Einführung intelligenter Verkehrssysteme[335] soll wesentlich dazu beitragen, die Sicherheit auf deutschen Straßen zu erhöhen und gleichzeitig den Verkehrsfluss steuern und optimieren zu können. Eine Einführung erscheint insbesondere im Hinblick auf eine optimale Nutzung von Straßen-, Verkehrs- und Reisedaten, eine Kontinuität der Dienste in den Bereichen Verkehrs- und Frachtmanagement und die Verbindung zwischen Fahrzeug und Infrastruktur sinnvoll.[336]

Damit diese Informationssysteme auch europaweit und somit grenzüberschreitend einsetzbar sind, ist es erforderlich, dass die technischen Voraussetzungen europaweit einheitlich festgelegt werden. Dies wird schon bedingt durch den gemeinsamen Markt.[337] Dazu ist es vor allem vorgesehen, dass die Europäische Kommission in den vorrangigen Bereichen[338] sog. Spezifikationen als delegierte Rechtsakte im Sinne des Art. 290 AEUV[339] erlässt, die dann bei der nationalen Einführung von Anwendungen und Diensten Intelligenter Verkehrssysteme zu beachten und vom Bundesministerium für Verkehr, Bau und Stadtentwicklung im Rahmen von Rechtsverordnungen umzusetzen[340] sind.[341] Auf nationaler Ebene existiert mittlerweile der sog. IVS-Aktionsplan *„Straße“*, der die Vorgehensweise für die Einführung und Weiterentwicklung Intelligenter Ver-

---

331 *Entwurf eines Gesetzes über Intelligente Verkehrssysteme im Straßenverkehr und deren Schnittstellen zu anderen Verkehrsträgern (Intelligente Verkehrssysteme Gesetz – IVSG) vom 19.02.2013*, vgl. BT-Drs. 17/12371 vom 19.02.2013.

332 BT-Drs. 17/12768 vom 14.03.2013, http://dip21.bundestag.de/dip21/btd/17/127/1712768.pdf.

333 BR-Drs. 256/13(B) vom 03.05.2013, http://dipbt.bundestag.de/dip21/brd/2013/0256-13B.pdf.

334 Die Veröffentlichung im Bundesgesetzblatt erfolgte am 20.06.2013, vgl. BGBl. I 2013, Nr. 29 vom 20.06.2013, S. 1553.

335 Vgl. unter *Kapitel 2, Teil 4*.

336 Vgl. ZD-Aktuell 2013, 03567.

337 BT-Drs. 17/12371 vom 19.02.2013, S. 7, http://dip21.bundestag.de/dip21/btd/17/123/1712371.pdf.

338 Als vorrangige Maßnahmen werden u.a. angesehen die Bereitstellung EU-weiter multimodaler Reise-Informationsdienste und Echtzeit-Verkehrsinformationsdienste, Verfahren zum unentgeltlichen Angebot relevanter Verkehrsmeldungen, die harmonisierte Bereitstellung einer interoperablen EU-weiten eCall-Anwendung, die Bereitstellung von Informationsdiensten für sichere Parkplätze für Lastkraftwagen sowie diesbezügliche Bereitstellung von Reservierungsdiensten, vgl. ZD-Aktuell 2013, 03567.

339 Vgl. Art. 7 IVS-RL.

340 Vgl. § 5 IVSG.

341 Vgl. Art. 6 IVS-RL sowie § 3 IVSG.

kehrssysteme definiert und einen Maßnahmenplan zu Zielen, Verantwortlichkeit und Etappen der einzelnen Maßnahmen enthält.[342] In diesem sollen die prioritären Regelungs- und Handlungsmaterien festgeschrieben werden, anhand derer die Einführung Intelligenter Verkehrssysteme erleichtert vollzogen werden soll. Zur optimalen Nutzung von Straßenverkehrs- und Reisedaten beispielsweise ist der Aufbau eines Mobilitäts Daten Marktplatzes (MDM) in Planung, im Rahmen dessen das LKW-Parken telematisch gesteuert werden kann.[343]

Aus datenschutzrechtlicher Sicht ist auch diese Entwicklung insgesamt zunächst noch kritisch zu hinterfragen. Es besteht mithin die Gefahr, dass bei der Anwendung Intelligenter Verkehrssysteme personenbezogene Daten erhoben und gespeichert werden. Da in diesem Zusammenhang viele Daten durch die Anwendung von Big Data erst generiert werden, kann zum jetzigen Zeitpunkt nicht vorausgesagt werden, welche Datensätze durch technische Weiterentwicklung noch entstehen können. Es bleibt auch abzuwarten, wie sich die Situation nach Erlass erster Spezifikationen durch die Europäische Kommission darstellt.

VII. Aktueller Stand und Ausblick

Zurzeit herrscht in Bezug auf das Gesetzgebungsverfahren für ein Gesetz zum Beschäftigendatenschutz weiterhin Stillstand. Die Verhandlungen zur Datenschutz-Grundverordnung konnten mittlerweile abgeschlossen und die Verordnung erlassen werden.

Das Inkrafttreten der Datenschutz-Grundverordnung und deren Anwendbarkeit ab dem 25.05.2018 werden wiederum Auswirkungen auf das Bundesdatenschutzgesetz haben. Bis zu diesem Zeitpunkt könnten bereits Spezifikationen im Sinne des Intelligente Verkehrssysteme Gesetz erlassen worden sein, was zudem Auswirkungen auf den nationalen Datenschutz haben wird.

---

342 Vgl. http://www.bmvi.de/SharedDocs/DE/Artikel/DG/ivs-im-strassenverkehr.html?linkToOverview=js.

343 Vgl. unter *Kapitel 2, Teil 4, II.3.*.

Teil 2: Die Anwendbarkeit des Bundesdatenschutzgesetzes

Das Bundesdatenschutzgesetz regelt seine Anwendbarkeit durch verschiedene Erlaubnistatbestände. Dabei müssen allerdings bei jeder Erhebung, Verarbeitung oder Nutzung allgemeine Grundsätze und Gebote berücksichtigt werden.

I. Datenschutzrechtliche Grundprinzipien

Die datenschutzrechtlichen Grundprinzipien sind nicht zwingend als selbständige Vorschriften ausgestaltet. Einzelne der Grundprinzipien sind von solch allgemeiner Natur, dass sie in einzelne Vorschriften hineingelesen werden bzw. von sich aus Allgemeingültigkeit besitzen.

1. Datenverarbeitung mit Erlaubnisvorbehalt

Nach der zentralen Norm des § 4 Abs. 1 BDSG sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Jede Datenverarbeitung bedarf mithin einer rechtlichen Rechtfertigung durch Einwilligung oder Erlaubnisnorm.[344] Als vorrangige Rechtsvorschriften kommen in diesem Zusammenhang auch die noch zu thematisierenden Betriebs- bzw. Dienstvereinbarungen in Betracht.[345]

2. Direkterhebung

Nach dem Gebot der Direkterhebung hat die Erhebung der Daten direkt beim Betroffenen zu erfolgen[346].

Als Voraussetzung einer Beschaffung beim Betroffenen selbst muss dies auf einer bewussten Mitwirkung durch aktives Tun oder passives Unterlassen des Betroffenen erfolgen.[347] Dass die Datenerhebung nur mit Kenntnis und unter Mitwirkung des Betroffenen erfolgt, ist eine entscheidende Voraussetzung für die effektive Ausübung sei-

---

344 Vgl. *Wolff* in Wolff/Brink: Datenschutzrecht in Bund und Ländern, 2013, Syst. A, Rn. 7
345 Vgl. *Gola/Klug*: Grundzüge des Datenschutzrechts, 2003, S. 48.
346 Vgl. § 3 Abs. 3 BDSG.
347 Vgl. *Weichert* in DKWW: Bundesdatenschutzgesetz, [4]2014, § 4, Rn. 6.

nes Rechts auf informationelle Selbstbestimmung.[348] Dazu treffen die verantwortliche Stelle sowohl Unterrichtungs- als auch Hinweis- und Aufklärungspflichten.[349]

Im Zusammenhang mit intelligenten Kraftfahrzeugen spielt insbesondere das heimliche Auslesen von sog. RFID[350]-Chips eine Rolle. Dies kann unter Anwendung des Gebots der Direkterhebung nicht mehr als bewusstes Mitwirken des Betroffenen gewertet werden.[351] Dies gilt auch, wenn der Betroffene weiß, dass sich ein solcher RFID-Chip im Fahrzeug befindet und dieser dazu geeignet wäre, ausgelesen zu werden.[352]

Zu diesem Gebot existieren jedoch einige Ausnahmen.[353]

Zum einen kann von einer Direkterhebung als notwendige Voraussetzung abgesehen werden, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt.[354] Letzteres ist dann der Fall, wenn im Sinne der Aufgabenerfüllung eine Datenerhebung verdeckt erfolgen müsste.[355] Versucht der Arbeitgeber z.B. eine mögliche Straftat eines Arbeitnehmers durch Datenerhebung aufzudecken, müsste befürchtet werden, dass dies seitens des Arbeitnehmers zu vereiteln versucht wird. Dies würde es insoweit rechtfertigen, die Daten nicht direkt beim Betroffen und unter Mitwirkung desselben zu beschaffen.

Zum anderen ist eine Ausnahme von dem Gebot der Direkterhebung dann anzunehmen, wenn die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht.[356] Dies gilt insbesondere dann, wenn z.B. die Vermutung besteht, ein Arbeitnehmer habe im Bewerbungsverfahren falsche oder nur unzureichende Angaben gemacht, sodass der Arbeitgeber sich der Hilfe Dritter bemühen muss, um dies durch weitere Datenerhebung zu hinterfragen.

---

348 Vgl. *Tinnefeld/Buchner/Petri*: Einführung in das Datenschutzrecht, [5]2012, S. 237.
349 Vgl. § 4 Abs. 3 BDSG.
350 „*Radio Frequency Identification*".
351 Vgl. *Taeger* in Taeger/Gabel: BDSG, [2]2013, § 4 BDSG, Rn. 62.
352 Vgl. *Bausewein,* 2012, S. 41.
353 Vgl. dazu insgesamt § 4 Abs. 2 BDSG.
354 Vgl. § 4 Abs. 2 Satz 2 Nr. 1 BDSG. Für den Fall einer dies vorsehendenden Rechtsvorschrift sei beispielhaft die Regelung des § 275 Abs. 1a Satz 3 SGB V erwähnt, nach der eine Arbeitsunfähigkeit eines Arbeitnehmers durch den Arbeitgeber ohne dessen Mitwirkung vom medizinischen Dienst seiner Krankenkasse überprüft werden kann.
355 Dies bezieht sich auf die Regelung des § 4 Abs. 2 Satz 2 Nr. 2 BDSG, vgl. *Taeger* in Taeger/Gabel: BDSG, [2]2013, § 4 BDSG, Rn. 67.
356 Vgl. § 4 Abs. 2 Satz 2 Nr. 2 lit. a BDSG.

Die vorgenannten Ausnahmetatbestände stehen kumulativ unter der Voraussetzung, dass keine Anhaltspunkte dafür bestehen, überwiegende schutzwürdige Interessen des Betroffenen würden beeinträchtigt.[357]

3. Datenvermeidung und Datensparsamkeit

Auch das Gebot der Datenvermeidung und Datensparsamkeit[358] ist im Rahmen der Datenverarbeitung zu beachten. Danach sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren[359] oder zu pseudonymisieren[360], soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert. Verlangt wird also eine datensparende Organisation, die darauf ausgerichtet sein soll, nur die für die Verarbeitung essentiellen Daten zu sammeln.[361] Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten soll durch Gestaltung der Systemstrukturen soweit wie möglich vermieden werden.[362] Das Ziel gilt als erreicht, wenn keine personenbezogenen Daten verarbeitet werden, wenn also der Personenbezug nicht gegeben ist, d.h. die Daten zumindest faktisch anonymisiert sind.[363]

4. Transparenz

Der Grundsatz der Transparenz soll verhindern, dass letztlich eine Datenverarbeitung sozusagen *„hinter dem Rücken“* des Betroffenen erfolgt. Dies ist jedoch nur zu gewährleisten, wenn der Betroffene über jegliche Datenerhebung und Datenverarbeitung umfassend informiert wird. Insoweit versteht sich der Grundsatz der Transparenz als

---

357 Vgl. § 4 Abs. 2 Satz 2 a.E. BDSG.

358 Vgl. § 3a BDSG.

359 Gemäß § 3 Abs. 6 BDSG meint das Anonymisieren das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

360 Gemäß § 3 Abs. 6a BDSG versteht man unter Pseudonymisieren das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

361 Vgl. *Tinnefeld/Buchner/Petri*: Einführung in das Datenschutzrecht, [5]2012, S. 238.

362 Vgl. *Gola/Klug*: Grundzüge des Datenschutzrechts, 2003, S. 46 f.; dort wird insoweit von Systemdatenschutz gesprochen.

363 Vgl. *Gola/Schomerus*: BDSG, [12]2015, § 3a, Rn. 6; eine Pseudonymisierung stellt hingegen nur eine relative Anonymität her, vgl. ebenda Rn. 10.

Aufgabe nicht nur bezüglich der Datenerhebung, sondern während der gesamten Dauer der Datenverarbeitung.[364]

5. Zweckbindung

Der auch in der Datenschutz-Grundverordnung festgeschriebene[365] Grundsatz der Zweckbindung ist an verschiedenen Stellen des Bundesdatenschutzgesetzes verankert.[366] Danach dürfen Daten von den verantwortlichen Stellen grundsätzlich nur zu dem Zweck verarbeitet und genutzt werden, zu dem sie erfasst worden sind.

In der Rechtsprechung wurde dieser Grundsatz vor allem im sog. *„Volkszählungsurteil"* des Bundesverfassungsgerichts zum Prüfungsmaßstab für die Datenverwendung erklärt, wonach es unzulässig sein soll, personenbezogene Daten ohne bestimmte Zweckbestimmung lediglich auf Vorrat zu sammeln.[367] Modifizierend hat das Bundesverfassungsgericht in seinem Urteil zur Vorratsdatenspeicherung vom 02.03.2010[368] klargestellt, dass eine anlasslose Speicherung von Telekommunikationsverkehrsdaten nicht zwangsläufig gegen den Zweckbindungsgrundsatz verstoße und somit nicht dem strikten Verbot einer Speicherung von Daten auf Vorrat unterfallen soll.[369]

Die Zweckbestimmung muss bereits zum Zeitpunkt der Datenerhebung feststehen und kann im weiteren Verlauf nur rechtmäßig geändert werden, wenn die Änderung mit der ursprünglichen Zweckbestimmung vereinbar ist.[370] Da es sich bei dem Zweckbindungsgrundsatz um einen echten Rechtssatz handelt, macht jeder Verstoß gegen denselben eine Maßnahme rechtswidrig.[371]

---

364 Vgl. *Roßnagel* in Roßnagel: Handbuch Datenschutzrecht, 2003, 1. Einleitung, Rn. 38.

365 Vgl. dazu insbesondere Art. 5 Abs. 1 lit. b) DS-GVO.

366 Vgl. u.a. §§ 4b Abs. 6, 4c Abs.1 Satz 2, 14 Abs. 1 Satz 1 und Abs. 2, 28 Abs. 1 Satz 2 und Abs. 2, 33 Abs. 1, 34 Abs. 1 Satz 1 Nr. 3 BDSG.

367 *„Die Verwendung der Daten ist auf den gesetzlich bestimmten Zweck begrenzt. Schon angesichts der Gefahren der automatischen Datenverarbeitung ist ein - amtshilfefester - Schutz gegen Zweckentfremdung durch Weitergabe- und Verwertungsverbote erforderlich", s*o das Bundesverfassungsgericht, Urteil vom 15.12.1983, Aktenzeichen 1 BvR 209/83, NJW 1984, S. 419-428 (422).

368 Bundesverfassungsgericht, Urteil vom 02.03.2010, Aktenzeichen 1 BvR 256/08, 263/08, 586/08, NJW 2010, S. 833-856; das Bundesverfassungsgericht entschied, dass die in Umsetzung der Richtlinie 2006/24/EG ergangenen §§ 113a, 113b TKG sowie § 100g StPO nicht mit dem Telekommunikationsgeheimnis nach Art. 10 Abs. 1 GG vereinbar seien.

369 Vgl. *Tinnefeld/Buchner/Petri*: Einführung in das Datenschutzrecht, ^{5}2012, S. 237.

370 Vgl. *Gola/Klug*: Grundzüge des Datenschutzrechts, 2003, S. 48; eine Zweckänderung ist zudem ausnahmsweise zulässig, soweit dies gesetzlich geregelt ist, wie z.B. in § 28 Abs. 2, 3 und 8 BDSG bezüglich der Übermittlung erhobener Daten.

371 Vgl. *Wolff* in Wolff/Brink: Datenschutzrecht in Bund und Ländern, 2013, Syst. A, Rn. 14

Im Zusammenhang mit intelligenten Kraftfahrzeugen spielt an dieser Stelle auch die Problematik von Profilbildung eine große Rolle. Wie bereits dargestellt[372], ist es aufgrund technischer Entwicklung und der Anwendung von Big Data bereits zum jetzigen Zeitpunkt aber insbesondere auch zukünftig ein Leichtes, ein Profil des Autofahrers aufzustellen. Grundsätzlich kann der dadurch entstehenden Gefahr für die informationelle Selbstbestimmung durch Hinweise in der Datenschutzerklärung bezüglich der Struktur und des Zweckes der Profilbildung begegnet werden.[373]

Zu beachten ist, dass der Zweckbindungsgrundsatz auch hinsichtlich der Verarbeitung von Beschäftigtendaten uneingeschränkte Gültigkeit besitzt und im Einzelfall stets auf die Erforderlichkeit abzustellen ist.[374] Der Grundsatz der Erforderlichkeit der Datenerhebung verlangt eine Beschränkung der Verarbeitung und Nutzung der Daten auf das notwendige Maß[375] sowie eine Abwägung der widerstreitenden Interessen im Einzelfall.[376] Eine Datenverarbeitung ist nur zulässig, soweit dies zur Erreichung des Zwecks notwendig ist. Somit muss die Datenverarbeitung im Rahmen einer kausalen Zweckförderung objektiv tauglich sein, den festgelegten Zweck zu erreichen bzw. die Zweckerreichung zu erleichtern.[377] Dies ist in jedem Einzelfall genau zu prüfen und zu hinterfragen.

II. Persönlicher Anwendungsbereich

In persönlicher Hinsicht schützt das Bundesdatenschutzgesetz den Betroffenen. [378] Der Schutzauftrag richtet sich hingegen an die sog. verantwortliche Stelle.

---

372 Vgl. unter *Kapitel 2, Teil 5, I.*.

373 Vgl. *Roßnagel* in Roßnagel: Handbuch Datenschutzrecht, 2003, 1. Einleitung, Rn. 42; auf diese Problematik wird jedoch im weiteren Verlauf insbesondere im Hinblick auf die sich durch die Anwendung von Big Data ergebenden Möglichkeiten noch näher einzugehen sein.

374 Vgl. *Bausewein,* 2012, S. 46.

375 Sog. Übermaßverbot.

376 Vgl. *Gola/Klug*: Grundzüge des Datenschutzrechts, 2003, S. 46.

377 Vgl. *Wolff* in Wolff/Brink: Datenschutzrecht in Bund und Ländern, 2013, Syst. A, Rn. 28.

378 Der Betroffene bildet den Mittelpunkt des Regelungsgefüges des Bundesdatenschutzgesetzes. Sein Persönlichkeitsrechtsschutz ist Zweck des Bundesdatenschutzgesetzes (§ 1 Abs. 1 BDSG), von seiner Einwilligung kann die Zulässigkeit einer Datenverwendung abhängen (§ 4 Abs. 1 BDSG), er kann durch Wahrnehmung seiner Rechte die Datenverarbeitung beeinflussen und kontrollieren (jeweils zweiter Unterabschnitt des zweiten und dritten Abschnitts) und er kann als Verletzter Strafantrag nach § 44 Abs. 2 BDSG stellen, vgl. *Dammann* in Simitis: Bundesdatenschutzgesetz, ^{8}2014, § 3, Rn. 40.

1. Betroffener

Der Begriff des Betroffenen ist legaldefiniert in der Vorschrift des § 3 Abs. 1 BDSG. Es handelt sich danach um eine bestimmte oder bestimmbare natürliche Person, deren Einzelangaben zu persönlichen oder sachlichen Verhältnissen verarbeitet werden.

Es ist Voraussetzung, dass es sich um Angaben handelt, die sich auf eine natürliche Person beziehen.[379] Juristische Personen und nichtrechtsfähige Personengruppen wurden seitens des Gesetzgebers absichtlich aus dem Anwendungsbereich ausgeklammert mit der Begründung, dass dieser Bereich kaum fassbar sei und die Praktikabilität der Gesetzesanwendung beeinträchtigen könnte.[380]

2. Verantwortliche Stelle

Unter dem Begriff der verantwortlichen Stelle werden alle Normadressaten zusammengefasst, die in § 2 BDSG aufgezählt sind. Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.[381]

Maßgeblich kommt es hierbei darauf an, wer die Entscheidungsgewalt über den Zweck und die Mittel der Datenverarbeitung hat.[382] Für die Verantwortlichkeit im Sinne des Bundesdatenschutzgesetzes kommt es mithin entscheidend auf die rechtliche und tatsächliche Entscheidungsbefugnis im Hinblick auf die Datenverwendung an.[383] Relevant ist, dass sich die Entscheidungsmöglichkeit nicht nur auf das *„Ob“*, sondern auch auf das *„Wie“* der Datenverarbeitung bezieht.[384]

Dabei ist es nicht erforderlich, dass die verantwortliche Stelle im Besitz der Daten ist oder die physische Herrschaft über den Verarbeitungsprozess ausübt, sodass auch im

---

379 Vgl. *Damann* in Simitis: Bundesdatenschutzgesetz, [8]2014, § 3, Rn. 17.

380 BT-Drs. 7/1027 vom 21.09.1973, S. 19 (Abschnitt 3.9.4.), http://dipbt.bundestag.de/doc/btd/07/010/0701027.pdf.

381 Vgl. § 3 Abs. 7 BDSG. Der Begriff der „*für die Verarbeitung Verantwortlichen*“ wird in Art. 2 lit. d DS-RL definiert als natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Dabei wird teilweise vertreten, beide Begriffen stimmten überein, vgl. *Buchner* in Taeger/Gabel: BDSG, [2]2013, § 3 BDSG, Rn. 52. Nach anderer Auffassung wird davon ausgegangen, dass der Begriff des Bundesdatenschutzgesetzes über den der Datenschutz-Richtlinie hinausgehe und dass deshalb eine richtlinienkonforme Auslegung zu erfolgen habe, vgl. *Plath/Schreiber* in Plath: BDSG, § 3, Rn. 66. Dieser Streit soll für die weitere Untersuchung jedoch nicht weiter relevant sein.

382 Vgl. *Jotzo*, MMR 2009, S. 232–237 (233).

383 Vgl. Tinnefeld/Buchner/Petri: Einführung in das Datenschutzrecht, [5]2011, S. 232.

384 So *Roßnagel*, SVR 2014, S. 281–287 (284).

Fall der Auslagerung zur Auftragsdatenverwaltung die Verantwortlichkeit bestehen bleibt.[385] Der Auftraggeber bleibt als Herr der Daten verantwortlich im Sinne des Bundesdatenschutzgesetzes.[386]

Bei vernetzen Fahrzeugen können unter Umständen einzelne Anwendungen unter den Anwendungsbereich des Telemediengesetzes fallen.[387] Auch im Anwendungsbereich des Telemediengesetzes ist die verantwortliche Stelle nach der Vorschrift des § 3 Abs. 7 BDSG zu bestimmen. Die spezialgesetzlichen Regelungen der §§ 7 ff. TMG beziehen sich lediglich auf die strafrechtliche Verantwortlichkeit und die Schadensersatzhaftung.[388] Mangels spezialgesetzlicher Regelungen ist mithin ein Rückgriff auf die Vorschriften des Bundesdatenschutzgesetzes vorzunehmen.

Im Zusammenhang mit vernetzten Kraftfahrzeugen können verschiedenen Akteure als verantwortliche Stelle eingestuft werden. Zunächst kann für die Anwendung von Telematik-Tarifen die Versicherung verantwortlich sein, die dem Versicherungsnehmer Boni gewährleistet, sofern dieser in sein Kraftfahrzeug eine Telematik-Box einbauen lässt, über die die entsprechenden Daten von einem externen Dritten an die Versicherung weitergeleitet werden. Aber auch der Hersteller von Kraftfahrzeugen ist als verantwortliche Stelle auszumachen hinsichtlich aller aus dem Kraftfahrzeug generierten Daten. Denn die Hersteller haben insoweit die Herrschaft und nahezu alleinige Kenntnis darüber, welche Daten erhoben und gespeichert werden. Aber auch Werkstätten können als verantwortliche Stelle angesehen werden, wenn diese die vorhandenen Daten für Fernwartung nutzen. Im Ergebnis ist mithin auf die jeweilige Maßnahme abzustellen und darüber zu ermitteln, wer aufgrund der Herrschaft über die jeweiligen Daten Zugriff auf dieselben hat und demnach als verantwortliche Stellen einzuordnen ist. Es muss hierbei mithin differenziert werden danach, wer welche Datenverarbeitung vornimmt.[389] Beim vernetzten Fahrzeug bestehen hierbei die soeben nicht abschließend dargestellten Fallgruppen. Zudem sind zahlreiche weitere Verantwortliche Stellen denkbar, die sich aus den speziellen Anwendungsbereichen im vernetzten Fahrzeug ergeben.

---

385 Vgl. *Dammann* in Simitis: Bundesdatenschutzgesetz, [8]2014, § 3, Rn. 225.
386 Vgl. *Gola/Schomerus*: BDSG, [12]2015, § 3, Rn. 50.
387 Vgl. unter *Kapitel 3, Teil 3, III.*.
388 Bundesgerichtshof, Urteil vom 23.06.2009, Aktenzeichen VI ZR 196/08, NJW 2009, S. 2888-2894 (2889) und Bundesgerichtshof, Urteil vom 27.03.2007, Aktenzeichen VI ZR 101/06, NJW 2007, S. 2558-2559 (2559).
389 So *Rieß/Greß*, DuD 2015, S. 391–396 (395).

Nach der Datenschutz-Grundverordnung besteht nunmehr auch die Kategorie der *„Gemeinsam für die Datenverarbeitung Verantwortliche(n)“*. Gemäß Art. 26 Abs. 1 DS-GVO sind mehrere Verantwortliche sog. Gemeinsam Verantwortliche, wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen. Dazu legen sie in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß der Datenschutz-Grundverordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht und wer welchen Informationspflichten gemäß Art. 13, 14 DS-GVO nachkommt.[390] Dabei kommt es besonders darauf an, dass die betroffene Person anhand der Vereinbarung die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen ihr gegenüber erkennen kann.[391] Besteht also aufgrund einer etwaigen komplexen und umfangreichen Datenverarbeitung eine Verantwortlichkeit mehrerer Stellen, wird zum Schutz des Betroffenen geregelt, dass sodann eine gemeinsame Verantwortlichkeit besteht. Somit kann auch eine Herrschaft über die Daten bei verschiedenen Stellen gleichzeitig bestehen, was jedoch letztlich dem Betroffenen gegenüber angezeigt werden muss.

Wenn also im Zusammenhang mit vernetzten Fahrzeugen die Datenverarbeitung aufgrund der technischen Ausgestaltung realitätsnah bei mehreren Verantwortlichen gleichzeitig erfolgt, darf dies dem Betroffenen nicht zum Nachteil gereichen.

III. Sachlicher Anwendungsbereich

Das Bundesdatenschutzgesetz regelt den Umgang mit personenbezogenen Daten[392] und gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten.[393] Der Umgang mit Daten ist als Oberbegriff für die Phasen des Erhebens, Speicherns, Veränderns, Übermittelns, Sperrens, Löschens und Nutzens zu verstehen.[394]

1. Personenbezogenes Datum

Nach der Legaldefinition des § 3 Abs. 1 BDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse[395] einer bestimmten oder bestimmbaren natürlichen Person. Obwohl der Gesetzeswortlaut ausschließlich von personenbe-

390 Vgl. Art. 26 Abs. 1 Satz 2 DS-GVO.
391 Vgl. Art. 26 Abs. 2 DS-GVO.
392 Vgl. § 1 Abs. 1 BDSG.
393 Vgl. § 1 Abs. 2 BDSG.
394 Vgl. *Gola/Schomerus*: BDSG, [12]2015, § 1, Rn. 22.
395 Die Formulierung entspricht dem Wortlaut des § 203 Abs. 2 Satz 2 StGB.

zogenen Daten im Plural spricht, erstreckt sich der Anwendungsbereich auch auf das einzelne personenbezogene Datum. Als Personenbezug bezeichnet man den Bezug eines Zustands oder eines Verhaltens zur Rechtssphäre einer Person, der sich auf einzelne oder eine Mehrzahl erkennbarer, bestimmter oder bestimmbarere Personen bezieht.[396]

Es sei vorangestellt, dass der Begriff der personenbezogenen Daten wegen der demgegenüber weiten Definition in Art. 2a DS-RL in Zweifelsfällen richtlinienkonform auszulegen ist.[397]

a) Einzelangabe über persönliche oder sachliche Verhältnisse

Zunächst muss es sich um eine Einzelangabe über persönliche oder sachliche Verhältnisse handeln. Von dem Begriff der Angabe ist jede Information umfasst mit der Einschränkung, dass ein finales, auf Vermittlung oder Aufbewahrung gerichtetes Element erforderlich ist.[398] Auch eine durch sog. *Scoring*[399] gewonnene Aussage, eine bestimmte Person gehöre zu einer nach bestimmten Kriterien zusammengestellten und bewerteten Gruppe, ist als Einzelangaben zu beurteilen.[400] Davon abzugrenzen sind jedoch die sog. aggregierten Daten als Zusammenfassung mehrerer Angaben.[401]

Des Weiteren muss die Angabe persönliche oder sachliche Verhältnisse betreffen. Dieses Tatbestandsmerkmal ist insgesamt umfassend zu verstehen und bezieht sich auf alle Informationen, die Aussagen über eine Person treffen. Auch das Bundesverfassungsgericht hielt bereits im Volkszählungsurteil fest, dass es *„unter den Bedingungen der automatischen Datenverarbeitung kein ´belangloses` Datum mehr“* gebe.[402] Einige Beispiele enthält das Bundesdatenschutzgesetz auch explizit.[403] Die persönlichen und sachlichen Verhältnisse umfassen ebenso Konsum- wie Freizeitaktivitäten, so z.B. Aufenthaltsangaben bzw. Standortdaten sowie als Namensersatz fungierende Angaben, die

---

396 Vgl. *Gusy* in Wolff/Brink: Datenschutzrecht in Bund und Ländern, 2013, § 1, Rn. 45, 47.

397 Vgl. *Plath/Schreiber* in Plath: BDSG, 2013, § 3, Rn. 6.

398 Vgl. *Dammann* in Simitis: Bundesdatenschutzgesetz, [8]2014, § 3, Rn. 5.

399 Dies betrifft auch die bereits zuvor genannte Score-Ermittlung der Sparkassen Direkt-Versicherung, vgl. unter *Kapitel 2, Teil 5, II.*.

400 Vgl. *Gola/Schomerus*: BDSG, [12]2015, § 3, Rn. 3a.

401 Darunter versteht man das Zusammenführen mehrerer personenbeziehbarer Datensätze zu einem Gruppendatensatz mit der Folge, dass nicht mehr festgestellt werden kann, welcher Person in einem Kollektivdatensatz welche Merkmale zugeordnet sind, vgl. *Weichert* in DKWW: Bundesdatenschutzgesetz, [4]2014, § 3, Rn. 47a.

402 Bundesverfassungsgericht, Urteil vom 15.12.1983, Aktenzeichen 1 BvR 209/83, NJW 1984, S. 419-428 (422).

403 So z.B. in § 28 Abs. 3 Satz 2 BDSG: *„(...) seine Berufs-, Branchen- oder Geschäftsbezeichnung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr (...)“*.

ausschließlich der Identifizierung dienen, wie beispielsweise das Kfz-Kennzeichen.[404] Auch die Fahrzeugidentifikationsnummer (FIN) liefert Informationen über persönliche oder sachliche Verhältnisse und fällt somit ebenfalls hierunter.

b) Bestimmtheit oder Bestimmbarkeit

Zusätzlich setzt die Anwendbarkeit des Bundesdatenschutzgesetzes die Bestimmtheit oder Bestimmbarkeit der Person voraus. Danach wird bemessen, ob ein Bezug zu einer einzigen Person hergestellt werden kann. Ansonsten besteht kein Schutz und die Daten stehen jedem zur freien Verfügung. Bestimmtheit liegt vor, wenn die Daten mit dem Namen des Betroffenen verbunden sind oder sich aus dem Inhalt bzw. dem Zusammenhang der Bezug unmittelbar herstellen lässt.[405] Ausreichend ist jedoch auch Bestimmbarkeit. Darunter fallen solche Informationen, die durch entsprechendes Zusatzwissen zugeordnet werden können.[406] Es müssen also Rückschlüsse auf die Person des Betroffenen möglich sein. Nach der Datenschutz-Grundverordnung soll kein Personenbezug mehr möglich sein, sofern die Daten anonymisiert sind.[407] Im Fall des Pseudonymisierens ist zu unterscheiden, ob der Betroffene das Pseudonym selbst generiert hat und somit eine Re-Identifizierung und deshalb auch eine Anwendbarkeit des Bundesdatenschutzgesetzes ausgeschlossen sind oder ob das Pseudonym von einer datenverarbeitenden Stelle zugeordnet und von dieser auch verwaltet wird.[408] Zur Feststellung der Bestimmbarkeit sind dabei alle Mittel zu berücksichtigen, die von dem für die Verarbeitung Verantwortlichen oder einer anderen Person aller Voraussicht nach zur Identifizierung der Person genutzt werden.[409]

Diskutiert wird in diesem Zusammenhang, ob das Merkmal der Bestimmbarkeit nach absoluten oder relativen Maßstäben zu bestimmen ist.

Nach der sog. relativen Theorie wird dabei ausschließlich auf die Kenntnisse und Möglichkeiten der datenverarbeitenden Stelle selbst abgestellt.[410] Dabei wird also der Begriff des Personenbezugs als relativ gesehen, wonach dieselben Daten der betroffenen Person aus der Sicht des Einen anonym und aus der Sicht des Anderen der betroffenen

404 Vgl. *Dammann* in Simitis: Bundesdatenschutzgesetz, [8]2014, § 3, Rn. 10, 11.
405 Vgl. *Gola/Schomerus*: BDSG, [12]2015, § 3, Rn. 10.
406 Vgl. *Tinnefeld* in Roßnagel: Handbuch Datenschutzrecht, 2003, 4.1 Geschützte Daten, Rn. 21.
407 Vgl. Erwägungsgrund (26) DS-GVO.
408 Vgl. *Tinnefeld/Buchner/Petri*: Einführung in das Datenschutzrecht, [5]2012, S. 228.
409 Vgl. Erwägungsgrund (26) DS-GVO; im Wesentlichen gleichen Inhalts ist dies in Erwägungsgrund (26) DS-RL geregelt.
410 Vgl. *Buchner* in Taeger/Gabel: BDSG, [2]2013, § 3 BDSG, Rn. 13.

Person zuordenbar sind.[411] Die relative Theorie wird dabei vom Bundesgerichtshof vertreten.[412]

Demgegenüber sollen nach der durch den Europäischen Gerichtshof[413] und die Art. 29-Datenschutzgruppe[414] vertretenen sog. absoluten Theorie objektive Maßstäbe angelegt werden und somit auch ein Personenbezug dadurch hergestellt werden können, wenn irgendein Dritter das hierfür nötige Zusatzwissen besitzt.[415]

Überzeugender ist hier jedoch, die Bestimmbarkeit als relativen Personenbezug zu deklarieren, indem dieselben Daten für den einen anonym und für den anderen der betroffenen Person zuzuordnen sind.[416] Es erscheint zu weitgehend, hier ein Zusatzwissen *„irgendeines"* Dritten ausreichen zu lassen. Vielmehr muss dazu auf die jeweilige verantwortliche Stelle abgestellt werden. Ob diese etwaiges Zusatzwissen über Dritte generieren kann, kann sodann im Anschluss überprüft werden. Jedoch kann nicht von vornherein die Verantwortlichkeit der betreffenden Stelle allein deshalb bejaht werden, weil ein Dritter Zusatzwissen besitzt. Insoweit ist hier für das Merkmal der Bestimmbarkeit auf die relative Theorie abzustellen.

c) Bestimmtheit oder Bestimmbarkeit im Bereich vernetzter Fahrzeuge

Die Problematik der Bestimmtheit bzw. Bestimmbarkeit stellt sich auch im Hinblick auf den Bereich der intelligenten Kraftfahrzeuge. Auch dort ist es entscheidend, ob die generierten Daten einer Person zugeordnet werden können, also letztlich personenbeziehbar sind. Dies spielt vor allem dann eine Rolle, wenn es sich um Daten handelt, die nicht auf den ersten Blick einen Personenbezug aufweisen, wie z.B. Messdaten.

(i) Position der Bundesregierung

Die Bundesregierung nahm aufgrund einer kleinen Anfrage der Fraktion Bündnis 90/Die Grünen[417] zu der Frage Stellung, wie personenbezogene Daten von fahrzeugbezogenen – und damit nicht personenbezogenen – Daten differenziert werden können:

---

411 Vgl. *Gola*: Datenschutz am Arbeitsplatz, [5]2014, Rn. 45.

412 Bundesgerichtshof, Beschluss vom 28.10.2014, Aktenzeichen VI ZR 135/13, GRUR Int. 2015, S. 296-300.

413 Europäischer Gerichtshof, Urteil vom 24.11.2011, Aktenzeichen C-70/10, MMR 2012, S. 174-176.

414 Vgl. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_de.pdf.

415 Vgl. *Buchner* in Taeger/Gabel: BDSG, [2]2013, § 3 BDSG, Rn. 13.

416 Vgl. *Gola/Schomerus*: BDSG, [12]2015, § 3, Rn. 10.

417 BT-Drs. 18/1166 vom 14.04.2014, http://dipbt.bundestag.de/doc/btd/18/011/1801166.pdf.

> *„Technische Messdaten in Fahrzeugsteuergeräten sind als solche zunächst nur*[418] *personenbeziehbar, ohne dass eine Verknüpfung mit der natürlichen Person des Fahrers unmittelbar erfolgt. Die Personenbeziehbarkeit auf einen bestimmten Fahrer wird im Einzelfall nur im Fall des Hinzutretens weiterer Ereignisse oder besonderer Umstände von Bedeutung (bspw. im Fall eines schweren Unfalls). Angesichts dieser Ausgangslage ist die faktische Bedeutung einer Herstellung des Personenbezuges im Alltag der Fahrzeugnutzer eingeschränkt.“*[419]

Die Bundesregierung sieht mithin keinen Handlungsbedarf. Sie unterscheidet zunächst zwischen Daten für Fahrzeugfunktionen und Daten für Servicefunktionen.[420] Die in Frage stehenden Messdaten sind hinsichtlich der gewählten Begrifflichkeiten der Bundesregierung als Daten für Fahrzeugfunktionen einzuordnen. Nach Ansicht der Bundesregierung ist die Schwelle zur Annahme von Personenbeziehbarkeit sehr hoch anzusetzen. Erst das Hinzutreten erheblicher Ereignisse könnte an diesem Grundsatz überhaupt etwas ändern. Die Relevanz solcher Daten ist danach faktisch nicht gegeben.

Dieser Auffassung ist aber mit Blick auf die Praxis entgegenzutreten. Dies greift zu kurz. Denn auch Daten für Fahrzeugfunktionen können bereits in alltäglichen Situationen Personenbezug aufweisen. Schon beim Auslesen eines Fehlerspeichers in einer Fachwerkstatt werden Messdaten erfasst, die sodann zusammen mit den sonstigen erhobenen Daten ein Bild des Fahrers und seiner Fahrweise zeichnen können. Dazu bedarf es nicht weiterer *„besonderer Umstände“*, weil es sich dabei insoweit um den alltäglichen Nutzen von Daten für Fahrzeugfunktionen handelt. Das Auslesen von Messdaten stellt entgegen der Darstellung der Bundesregierung wiederkehrende Situationen für den Fahrer dar. Die Messdaten sind für ihn bereits im Rahmen der Fehleranzeige im Kraftfahrzeug von Bedeutung. Es kann also letztlich nicht pauschal unterstellt werden, Messdaten seien im Alltag der Fahrzeugnutzer faktisch nicht von Bedeutung.

Dazu sei bekräftigend auf Art. 4 Nr. 1 DS-GVO verwiesen, wonach ein Personenbezug *„direkt oder indirekt“* hergestellt werden kann. Dies belegt, dass auch die sog. Daten für Fahrzeugfunktionen und somit Messdaten gerade auch Personenbezug aufweisen

---

418 Es muss vermutet werden, dass es sich hier um einen redaktionellen Fehler handelt und an dieser Stelle zunächst festgestellt werden sollte, dass technische Messdaten (…) grundsätzlich *„nicht“* personenbeziehbar sind.

419 BT-Drs. 18/1362 vom 02.05.2014, S. 5, http://dipbt.bundestag.de/dip21/btd/18/013/1801362.pdf.

420 BT-Drs. 18/1362 vom 02.05.2014, S. 2, http://dipbt.bundestag.de/dip21/btd/18/013/1801362.pdf.

können. Denn auch diese Daten lassen sich ohne größeren Aufwand dem Fahrer oder Halter zuordnen.

Die Ansicht der Bundesregierung überrascht jedoch im Hinblick auf eine zuvor an sie gestellte kleine Anfrage nicht. Auf die Frage, wie verhindert werden könne, dass Bewegungsprofile und Halterinformationen vernetzter Fahrzeuge ungehindert gespeichert und verarbeitet werden, lautete die Antwort der Bundesregierung:

„Die Bundesregierung hat diese Frage noch nicht vertieft geprüft.“[421]

Insoweit muss festgestellt werden, dass die Bundesregierung die Problematik der Personenbeziehbarkeit im Hinblick auf vernetzte Fahrzeuge noch nicht umfänglich erörtert und bislang die Rechtslage falsch eingeordnet hat. Ein Personenbezug kann mithin nicht nur bei offensichtlich personenbezogenen Daten vorliegen, sondern vielmehr auch bei Daten für Fahrzeugfunktionen, die auf den ersten Blick scheinbar lediglich technische Informationen liefern.

Dies bestätigt auch eine gemeinsame Stellungnahme der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA) zum Thema *„Datenschutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge“* vom 26.01.2016. In Bezug auf die Personenbezogenheit wird von dort ebenso festgestellt, dass im modernen Fahrzeug die anfallenden Daten bei Hinzuziehung weiterer Informationen auf den Halter oder auch auf den Fahrer und Mitfahrer zurückführbar sein und Informationen über persönliche oder sachliche Verhältnisse einer bestimmbaren Person enthalten können, sodass Daten jedenfalls dann Personenbezug aufweisen, wenn eine Verknüpfung mit der FIN oder dem Kfz-Kennzeichen vorliege.[422]

(ii) Prognosedaten

Wenn man mit der hier vertretenen Auffassung davon ausgeht, dass auch auf den ersten Blick belanglose Daten Personenbezug aufweisen können, stellt sich im Zusammenhang mit der vorliegenden Problematik die Frage, ob es aufgrund von Big Data-Anwendungen möglich sein kann, Vorhersagen über menschliches Verhalten zu treffen. Im Hinblick auf intelligente Kraftfahrzeuge soll es künftig möglich sein, eine Prognose

421 BT-Drs. 18/706 vom 05.03.2014, S. 11, http://dip21.bundestag.de/dip21/btd/18/007/1800706.pdf.

422 Vgl. https://www.vda.de/de/themen/innovation-und-technik/vernetzung/gemeinsame-erklaerung-vda-und-datenschutzbehoerden-2016.html.

darüber aufzustellen, ob bzw. wann ein Fahrer einen Unfall verursachen wird.[423] Auch solche Daten enthalten aber Angaben über in der Zukunft liegende Verhältnisse, auch wenn deren Realisierung noch ungewiss ist und beschreiben deshalb schon Verhältnisse des Betroffenen.[424] Für den Fall, dass Werkstätten oder Versicherer solche Prognosen zukünftig erstellen sollten, wären folglich auch diese Daten vom Anwendungsbereich des Bundesdatenschutzgesetzes umfasst.

Hinsichtlich einer Kfz-Werkstatt ist weiter zu differenzieren. Für den Fall, dass im Rahmen einer Diagnose Messdaten erhoben werden, sind diese als personenbezogene Daten einzuordnen, während dies nicht für beispielsweise aus einer Datenbank des Herstellers bezogene typenbedingte Kfz-Merkmale gilt.[425] Typenbedingte Angaben sind reine Sachangaben. Der Personenbezug wird hier erst dadurch hergestellt, dass im Rahmen der Diagnose sämtliche relevante Daten ausgelesen werden und dabei z.B. auch der persönliche Fahrstil des Fahrers sich wiederspiegeln kann.

Ähnlich stellt sich dies auch bezüglich geographischer Standortdaten bzw. Positionsdaten dar. Über GPS-Ortung[426] kann bereits jetzt jeder Standort eines Fahrers ermittelt werden. Die reinen GPS-Koordinaten sind insoweit mit den soeben genannten Daten aus der Datenbank eines Kfz-Herstellers zu vergleichen. Allein anhand derer lässt sich kein Personenbezug herstellen. Werden diese Daten jedoch mit weiteren personenbezogenen Daten und Informationen verknüpft, sind auch sie als personenbezogene Daten anzusehen.[427] Denn dadurch kann es z.B. möglich sein, einen Aufenthalts- oder Unfallort zu lokalisieren. Deshalb sind die Daten hier für einen potenziellen Unfallverursacher datenschurzrechtlich relevant, weil sie einen Personenbezug zu ihm herzustellen vermögen. Insoweit ist eine vorschnelle Ablehnung der Personenbeziehbarkeit technischer Daten zu kritisieren, weil unschwer eine Verknüpfung derartiger Daten mit der Fahrzeug-Identifikationsnummer oder dem Fahrzeug-Kennzeichen möglich ist.[428]

2. Besondere Arten personenbezogener Daten

Im Hinblick auf die Möglichkeiten, die durch die Technik in intelligenten Fahrzeugen bestehen bzw. zukünftig bestehen werden, müssen auch die besonderen Arten perso-

423 Vgl. unter *Kapitel 2, Teil 2, I.2.b)*.
424 Vgl. *Gola/Schomerus*: BDSG, [12]2015, § 3, Rn. 9.
425 Vgl. *Dammann* in Simitis: Bundesdatenschutzgesetz, [8]2014, § 3, Rn. 60.
426 Vgl. unter *Kapitel 2, Teil 2, I.2.b)*.
427 Vgl. *Dammann* in Simitis: Bundesdatenschutzgesetz, [8]2014, § 3, Rn. 69.
428 Vgl. *Schwartmann*, Sonderveröffentlichung zu RDV 3/2015, S. 6.

nenbezogener Daten beachtet werden. Diese sind katalogartig in § 3 Abs. 9 BDSG aufgeführt. Die dortige Aufzählung ist als abschließend anzusehen.[429] Bei diesen sensitiven Daten handelt es sich um solche, denen bei ihrer Erhebung, Verarbeitung und Nutzung diskriminierende Wirkung zukommen kann, sodass ein fehlerhafter Umgang mit diesen auch die Vermutung einer Diskriminierung begründen kann.[430]

Von diesen sog. sensitiven Daten sollen für die vorliegende Untersuchung lediglich die Angaben über die Gesundheit als Gesundheitsdaten Relevanz besitzen, da bereits Fahrerassistenzsysteme bestehen bzw. in der Entwicklung sind, die aufgrund von erhobenen Gesundheitsdaten eine Empfehlung an den Fahrer geben und diesem assistieren.[431]

Für die besonders geschützten Daten besteht im Rahmen der Einwilligungserteilung[432] und bei vorzunehmenden Abwägungsvorgängen[433] ein besonderer Schutz.[434] Auch hierbei kann durch Verknüpfung von Informationen über bestimmte Gegebenheiten, die an sich nicht als sensitiv zu bewerten sind, mit weiteren Daten bei der Qualifizierung als sensitive Daten eine Rolle spielen.[435]

Insoweit wurde bereits schon angesprochen[436], dass Kraftfahrzeuge in Zukunft mit medizinischen Sensoren ausgerüstet sein sollen, die Atemalkoholpegel oder Herzfunktion sowie psychische Verfassung messen. Ein etwaiger Alkoholkonsum an sich stellt beispielsweise zunächst kein Gesundheitsdatum dar.[437] Wird allerdings die Atemalkoholkonzentration von den jeweiligen Sensoren für jeden Einzelfall erhoben und eventuell im Kraftfahrzeug gespeichert, könnte dies im schlimmsten Fall auf eine Alkoholabhängigkeit hindeuten und würde letztlich mittelbar wiederum ein gesundheitliches Datum darstellen. Gegenüber diesem Extrembeispiel gilt Gleiches jedoch ebenfalls beispielsweise für eine durch medizinische Sensoren feststellbare Müdigkeit. Sofern durch Messungen der Herzfunktion oder aber auch der psychischen Verfassung und der Verknüpfung der daraus gewonnenen Daten darauf geschlossen werden kann, dass der Fahrer übermüdet am Steuer saß und ein etwaiger Unfall hierauf zurückzuführen sein könnte,

---

429 Vgl. *Buchner* in Taeger/Gabel: BDSG, [2]2013, § 3 BDSG, Rn. 59.
430 Vgl. *Buchner* in Wolff/Brink: Datenschutzrecht in Bund und Ländern, 2013, § 3, Rn 149.
431 Vgl. unter *Kapitel 2, Teil 2, I.2.b).*
432 Für eine wirksame Einwilligung ist eine besondere und vor allem ausdrückliche Bezugnahme auf die besonders geschützten Daten erforderlich, vgl. § 4a Abs. 3 BDSG.
433 Vgl. §§ 13 Abs. 2, 28 Abs. 6 bis Abs. 9, 29 Abs. 5 BDSG.
434 Vgl. Weichert in DKWW: Bundesdatenschutzgesetz, [4]2014, § 3, Rn. 65.
435 Dies betrifft u.a. Angaben über einen Arztbesuch oder den Gesundheitszustand; vgl. *Plath/Schreiber* in Plath: BDSG, 2013, § 3, Rn. 78.
436 Vgl. unter *Kapitel 2, Teil 2, I.2.b).*
437 Vgl. *Simitis* in Simitis: Bundesdatenschutzgesetz, [8]2014, § 3, Rn. 265.

ist auch dieses gesundheitliche Datum für den Fahrer und Versicherungen von höchster Relevanz.

3. Geschützte Art der Verarbeitung

Alle Phasen der Datenverarbeitung werden im Bundesdatenschutzgesetz unter dem Oberbegriff des *„Umgangs“*[438] zusammengefasst. Die als Generalklausel ausgestaltete Regelung des § 1 Abs. 1 BDSG zum *„Umgang“* mit personenbezogenen Daten umfasst alle im Gesetz vorgesehenen Formen der Verarbeitung personenbezogener Daten.[439]

Im Rahmen des Bundesdatenschutzgesetzes gilt ein engerer Verarbeitungsbegriff, der darunter das Speichern, Verändern, Übermitteln, Sperren und Löschen fasst.[440] Insoweit stellt die Veränderung als Unterfall der Verarbeitung personenbezogener Daten für den Datenschutz im Hinblick auf vernetzte Kraftfahrzeuge eine wichtige Tatbestandsalternative dar. Denn die Verknüpfung verschiedener Daten spielt insbesondere im Rahmen von Big Data-Anwendungen eine große Rolle.[441] Auch die bereits aufgeführte Score-Berechnung bei Telematik-Tarifen[442] ist hier als Veränderung und nicht als Nutzung der personenbezogenen Daten anzusehen. Die Änderung ist darin zu sehen, dass Daten mit einem bestimmten Informationsgehalt, d.h. dem Verhalten in der Vergangenheit, ein neuer Informationsgehalt in Gestalt des Verhaltens in der Zukunft beigemessen wird.[443]

Die Erhebung meint das Beschaffen von Daten über den Betroffenen.[444] Dabei ist die Art und Weise der Beschaffung unerheblich, sodass sowohl eine mündliche Abfrage als auch ein heimliches Beobachten ausreichend sind. Allerdings wird auch hier ein zielgerichtetes Handeln der erhebenden Stelle verlangt.[445] Die erhebende Stelle muss somit sowohl Kenntnis von den betreffenden Daten als auch Verfügungsgewalt über diese erhalten.[446] Bei der Einrichtung eines technischen Gerätes zum Empfang von Informati-

---

438 Vgl. § 1 Abs. 1 BDSG, wonach es der Zweck des Bundesdatenschutzgesetzes ist, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

439 Darunter fallen die Erhebung nach § 3 Abs. 3 BDSG, die Verarbeitung nach § 3 Abs. 4 BDSG sowie die Nutzung nach § 3 Abs. 5 BDSG, vgl. *Gusy* in Wolff/Brink: Datenschutzrecht in Bund und Ländern, 2013, § 1, Rn. 51

440 Vgl. § 3 Abs. 4 Satz 1 BDSG.

441 Vgl. unter *Kapitel 2, Teil 5*.

442 Vgl. unter *Kapitel 2, Teil 5, II.*

443 Vgl. *Buchner* in Taeger/Gabel: BDSG, [2]2013, § 3 BDSG, Rn. 32.

444 Vgl. § 3 Abs. 3 BDSG.

445 Landesarbeitsgericht Hamm, Beschluss vom 16.09.2011, Aktenzeichen 10 TaBV 17/11, ZD 2012, S. 183-186.

446 Vgl. *Dammann* in Simitis: Bundesdatenschutzgesetz, [8]2014, § 3, Rn. 102.

onen ist es erforderlich, dass dies zielgerichtet erfolgt und voraussetzt, dass die ohne weiteres Zutun erlangten Daten der erhebenden Stelle zugeordnet werden können.[447]

Bei dem Einbau beispielsweise eines Mobiltelefons in ein Dienstfahrzeug, das dem Arbeitnehmer insoweit zur Benutzung zur Verfügung steht, ist davon auszugehen, dass dies zielgerichtet zur Erlangung von Daten erfolgt und deshalb der erhebenden Stelle zuzuordnen ist. Da das Erheben von personenbezogenen Daten eine eigenständig geschützte Art der Datenverarbeitung darstellt, ist dieser Tatbestand ebenfalls erfüllt, wenn die Daten im weiteren Verlauf anonymisiert werden.[448]

Teil 3: Die Zulässigkeit der Datenverwendung im Beschäftigtendatenschutz

Die Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung[449] richtet sich zunächst nach der Vorschrift des § 4 BDSG.[450] Jede Datenverwendung ist danach grundsätzlich unzulässig, soweit sie nicht durch einen gesetzlichen Erlaubnistatbestand oder eine Einwilligung gedeckt ist. Die Datenverwendung unterliegt mithin einem Verbot mit Erlaubnisvorbehalt. Dies folgt zwangsläufig aus der Notwendigkeit, dass Eingriffe in das Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG einer rechtlichen Legitimation bedürfen.[451] Dieses Verbotsprinzip findet sich ebenfalls in Art. 8 Abs. 2 EU-GRCH sowie Art. 7 DS-RL und ist auch in Art. 6 DS-GVO vorgesehen.

Ein Anspruch auf den Schutz seines Persönlichkeitsrechts steht nach § 75 Abs. 2 BetrVG auch dem Arbeitnehmer zu. Es ist für jede einzelne Phase der Datenverwendung gesondert zu prüfen, ob die Voraussetzungen eines Erlaubnistatbestandes vorliegen.[452] Ist die jeweilige Datenverwendung nicht durch einen Erlaubnistatbestand gedeckt, ist diese rechtswidrig und der Betroffene kann Unterlassung oder Beendigung der Datenverwendung verlangen.[453]

---

447 Vgl. *Weichert* in DKWW: Bundesdatenschutzgesetz, [4]2014, § 3, Rn. 31.
448 Vgl. *Gola/Schomerus*: BDSG, [12]2015, § 3, Rn. 24.
449 Die Datenerhebung, -verarbeitung und –nutzung werden unter dem Begriff der Datenverwendung zusammengefasst und geführt.
450 An dieser Stelle soll die Zulässigkeit der Datenverwendung kurz dargestellt werden. Problematische Aspekte werden im weiteren Verlauf näher erörtert.
451 So *Karg*, DuD 2013, S. 75-79 (78).
452 Vgl. *Gola/Schomerus*: BDSG, [12]2015, § 4, Rn. 5.
453 Vgl. *Bäcker* in Wolff/ Brink: Datenschutzrecht in Bund und Ländern, 2013, § 4, Rn. 21.

Gesetzliche Erlaubnistatbestände können sich im Bundesdatenschutzgesetz selbst finden oder aber in sog. *„anderen Rechtsvorschriften“*. Im Rahmen der Erlaubnis durch eine andere Rechtsvorschrift ist im Hinblick auf den Beschäftigtendatenschutz das Vorliegen einer Betriebsvereinbarung zu problematisieren. Zudem stellt sich im Zusammenhang mit vernetzten Kraftfahrzeugen die Frage, ob in den Vorschriften des Intelligente Verkehrssysteme Gesetzes *„andere Rechtsvorschriften“* im Sinne des § 4 Abs. 1 BDSG zu sehen sind, die sodann eine Datenverarbeitung unter den dort aufgestellten Voraussetzungen zulassen. Auch bezüglich einer Einwilligung sind hier die Besonderheiten im Beschäftigtenverhältnis einerseits sowie solche, die sich andererseits aus der Technik der vernetzten Kraftfahrzeuge ergeben, zu beachten.

Unabhängig vom Inhalt der jeweiligen Vorschriften stellt sich jedoch die Frage, ob ein etwaiger Erlass arbeitsrechtlicher Vorschriften durch die Europäische Union im Rahmen der Datenschutz-Grundverordnung überhaupt kompetenzrechtlich möglich wäre.

Die Europäische Kommission stützt ihre Kompetenz bezüglich der Datenschutz-Grundverordnung jedenfalls auf Art. 16 Abs. 2 AEUV und Art. 114 Abs. 1 AEUV.[454] Allerdings regelt Art. 16 Abs. 2 AEUV die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten. Eine Datenverwendung durch Private ist hiervon nicht umfasst. Auch Art. 114 Abs. 1 AEUV kann insoweit nicht als Kompetenzgrundlage herangezogen werden. Diese allgemeine Vorschrift zur Rechtsangleichung im Binnenmarkt gilt ausdrücklich gerade nicht für *„die Bestimmungen über die Rechte und Interessen der Arbeitnehmer“*.[455]

Im Gegensatz zu den Regelungen der Datenschutz-Richtlinie enthält die Datenschutz-Grundverordnung nicht mehr nur sich als Annex auf das Arbeitsrecht auswirkende Bestimmungen, sondern tatsächlich genuine Regelungen zu den Rechten und Interessen der Arbeitnehmer mit der Folge, dass also lediglich die Möglichkeit besteht, als Kompetenzgrundlage auf die sozialpolitische Vorschrift des Art. 153 AEUV zurückzugrei-

---

454 *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) vom 25.01.2012*, KOM (2012) 11 endg., S. 6, http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM%282012%290011_DE.pdf.

455 Vgl. Art. 114 Abs. 2 AEUV.

fen.[456] Danach können das Europäische Parlament und der Rat zu den in Art. 153 Abs. 1 AEUV genannten Zwecken Maßnahmen zur Förderung der Zusammenarbeit annehmen.

Allerdings ist dies nur unter Ausschluss jeglicher Harmonisierung der Vorschriften der Mitgliedsstaaten erlaubt. Daraus folgt, dass die Datenschutz-Grundverordnung nur eine Mindestharmonisierung des Beschäftigtendatenschutzes vorsehen kann. Der Erlass einer Datenschutz-Grundverordnung mit vollharmonisierender Wirkung würde hingegen die Kompetenzen der Europäischen Union übersteigen. Aus der nunmehr erlassenen Datenschutz-Grundverordnung ergibt sich jedoch lediglich eine Mindestharmonisierung.[457]

I. Gesetzliche Erlaubnistatbestände nach § 4 BDSG

Gesetzliche Erlaubnistatbestände für eine ordnungsgemäße Datenverwendung können sich gemäß § 4 Abs. 1 BDSG entweder aus dem Bundesdatenschutzgesetz selbst oder aber aus anderen Rechtsvorschriften ergeben.

Auch die Datenschutz-Grundverordnung enthält Regelungen, die als gesetzliche Erlaubnistatbestände ausgestaltet sind. Diese finden sich in den Art. 5 – 11 DS-GVO. Die dort gewählten Formulierungen entsprechen größtenteils den bereits aus dem nationalen Recht bekannten Regelungen.

Grundsätzlich muss eine Datenverarbeitung danach auf rechtmäßige Weise und nach Treu und Glauben erfolgen.[458] Ebenso dürfen personenbezogene Daten nur für einen genau festgelegten, eindeutigen und rechtmäßigen Zweck erhoben werden.[459] Die Datenverarbeitung muss grundsätzlich dem Zweck angemessen, sachlich relevant und auf das notwendige Mindestmaß beschränkt werden.[460] Insoweit ist ebenfalls die Verhältnismäßigkeit zu wahren. Die vorgenannten Aspekte sind im Rahmen jeder Datenverarbeitung zu beachten. In Art. 6 DS-GVO sind schließlich Anforderungen an die Rechtmäßigkeit einer Datenverarbeitung festgeschrieben, die Bedingung für eine rechtmäßige Datenverarbeitung vorsehen. Als gesetzliche Erlaubnistatbestände finden sich dort u.a.

---

456 So *Franzen*, RDV 2014, S. 200–202 (201).

457 Vgl. Art. 86 DS-GVO, wonach die Mitgliedsstaaten in den Grenzen der Verordnung die Verarbeitung personenbezogener Arbeitnehmerdaten im Beschäftigungskontext für die dort genannten Zwecke regeln können.

458 Vgl. Art. 5 Abs. 1 lit. a DS-GVO.

459 Vgl. Art. 5 Abs. 1 lit. b DS-GVO.

460 Vgl. Art. 5 Abs. 1 lit. c DS-GVO.

die Erforderlichkeit zur Erfüllung eines Vertrages[461] oder zur Erfüllung einer rechtlichen Verpflichtung[462]. Auch zur Wahrnehmung im öffentlichen Interesse liegender Aufgaben[463] kann eine Datenverarbeitung rechtmäßig sein. Insoweit finden sich hier die aus dem Bundesdatenschutzgesetz bekannten Formulierungen wieder.

1. Die Erlaubnis zur Datenverwendung durch das Bundesdatenschutzgesetz selbst

Im Bundesdatenschutzgesetz existieren für verschiedene Bereiche Erlaubnistatbestände zur Datenverwendung. Diese finden sich in § 6b BDSG, in den §§ 13 ff. BDSG für öffentliche Stellen[464] und in den §§ 28 ff. für nicht-öffentliche Stellen.[465] Für die Datenverwendung aus vernetzten Fahrzeugen und im Zusammenhang mit Arbeitsverhältnissen sind hierbei insbesondere die Erlaubnistatbestände der §§ 28, 32 BDSG zu beachten, um eine Verarbeitung von Daten rechtfertigen zu können.

a) § 28 Abs. 1 Satz 1 Nr. 1 BDSG

So ist im vorliegenden Zusammenhang insbesondere der Erlaubnistatbestand für die Datenverwendung zur Vertragserfüllung im Rahmen eines Schuldverhältnisses von Relevanz. In Umsetzung des Art. 7 lit. b DS-RL regelt der Erlaubnistatbestand des § 28 BDSG zunächst die Zulässigkeit der Datenerhebung und Datenspeicherung für eigene Geschäftszwecke.[466]

Als rechtsgeschäftliches Schuldverhältnis im Sinne des § 28 BDSG gilt auch ein Beschäftigungsverhältnis. Dem Arbeitgeber ist es demnach erlaubt, auf dieser Grundlage

---

461 Vgl. Art. 6 Abs. 1 lit. b DS-GVO.

462 Vgl. Art. 6 Abs. 1 lit. c DS-GVO.

463 Vgl. Art. 6 Abs. 1 lit. e DS-GVO.

464 Die vorgenannten Tatbestände werden im Rahmen der vorliegenden Untersuchung nicht weiter behandelt. Relevant sind hier die Tatbestände der § 28 und § 32 BDSG hinsichtlich des Beschäftigtendatenschutzes.

465 Die hier behandelten Erlaubnistatbestände sollen kurz dargestellt werden. Eine tiefergehende Erörterung findet im weiteren Verlauf an entsprechender Stelle statt, so z.B. hinsichtlich der Ortung von Kraftfahrzeugen unter *Kapitel 3, Teil 7, III.2.*.

466 Danach ist die Datenverwendung personenbezogener Daten für die Erfüllung eigener Geschäftszwecke nach § 28 Abs. 1 Satz 1 BDSG zulässig, wenn es für eine Phase eines rechtsgeschäftlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist (Nr. 1), soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich und kein Grund ersichtlich ist, dass schutzwürdige Interessen des Betroffenen überwiegen (Nr. 2) oder wenn es sich um allgemein zugängliche Daten handelt, soweit nicht schutzwürdige Interessen des Betroffenen entgegenstehen (Nr. 3), vgl. § 28 Abs. 1 BDSG.

alle Daten zu verarbeiten, die im Rahmen der Zweckbestimmung des Beschäftigungsverhältnisses entstehen.[467]

Erlaubt ist nach § 28 Abs. 2 BDSG auch die Übermittlung oder Nutzung für andere Zwecke unter den dort genannten Voraussetzungen.[468]

(i) Erfüllung eigener Geschäftszwecke

Die Erfüllung eigener Geschäftszwecke nach § 28 Abs. 1 Satz 1 BDSG setzt voraus, dass die Datenverwendung als Mittel zum Zweck, also zur Erreichung eines dahinterstehenden Geschäftszweckes dient und gerade nicht selbst als geschäftliches Interesse gilt.[469] Die Datenverwendung darf also nicht den Hauptzweck darstellen. Vielmehr darf dies lediglich hilfsweise erfolgen, um den eigentlichen Hauptweck – die Abwicklung des rechtsgeschäftlichen Schuldverhältnisses – zu erfüllen. Zudem ist ein unmittelbarer sachlicher Zusammenhang zwischen der beabsichtigte Verwendung der Daten und dem konkreten Zweck des rechtsgeschäftlichen Schuldverhältnisses zu fordern.[470]

Innerhalb der drei Zulässigkeitsalternativen des § 28 Abs. 1 BDSG stellt sich bei Vorliegen eines rechtsgeschäftlichen Schuldverhältnisses dabei allerdings die Frage, ob die Zulässigkeitsalternativen tatsächlich nebeneinander anwendbar sind. Dies muss hier im Ergebnis abgelehnt werden. Obwohl sich die drei Zulässigkeitsalternativen generell gleichrangig gegenüber stehen, sind sie gerade nicht nebeneinander anwendbar. Die verantwortliche Stelle kann die Datenverwendung nur auf jeweils eine der drei Zulässigkeitsalternativen stützen.[471]

Deshalb ist in diesem Zusammenhang die Auffassung überzeugend, im Falle des Vorliegens eines rechtsgeschäftlichen Schuldverhältnisses die Zulässigkeit der Datenverwendung ausschließlich an den Voraussetzungen des § 28 Abs. 1 Satz 1 Nr. 1 BDSG zu

---

467 Vgl. *Büllesbach* in Roßnagel: Handbuch Datenschutzrecht, 2003, 6.1 Datenschutz in der betrieblichen Datenverarbeitung, Rn. 12.

468 Dies ist der Fall bei Erfüllung der soeben genannten Tatbestände des § 28 Abs. 1 Satz 1 Nr. 2 oder Nr. 3 BDSG (Nr. 1), soweit es zur Wahrung berechtigter Interessen oder zur Abwehr von Gefahren für die staatliche oder öffentliche Ordnung erforderlich ist und keine schutzwürdigen Interessen des Betroffenen entgegenstehen (Nr. 2 lit. a und b) oder wenn dies für die wissenschaftliche Forschung erforderlich ist.

469 Vgl. *Gola/Schomerus*: BDSG, [12]2015, § 28, Rn. 4.

470 Vgl. *Simitis* in Simitis: Bundesdatenschutzgesetz, [8]2014, § 28, Rn. 57.

471 Vgl. *Wedde* in DKWW: Bundesdatenschutzgesetz, [4]2014, § 28, Rn. 14.

messen und an dem Vertragszweck zu orientieren.[472] Ansonsten hätte es letztlich keine Bedeutung mehr, dass insoweit eine Spezialregelung vorhanden ist.

Vielmehr muss hier eine restriktive Auslegung erfolgen. Es kann nicht hingenommen werden, dass im Zweifel Datenverwendungen möglich sind, die über den Vertragszweck hinausgehen oder diesem gar entgegenstehen, nur weil dies der Wahrung berechtigter Interessen dient oder es sich um allgemein zugängliche Daten handelt. Auch *Wedde* äußert sich dahingehend, dass bei Vorliegen eines Schuldverhältnisses durch einen Rückgriff auf die Erlaubnistatbestände der Nr. 2 und Nr. 3 nicht mehr gestattet werden könne, als dies Nr. 1 erlauben würde.[473]

Die hier vertretene enge Auslegung der Vorschriften des § 28 Abs. 1 Satz 1 Nr. 2 und Nr. 3 BDSG hat auch das Bundesarbeitsgesetz bereits bestätigt. Nach Auffassung des Bundesarbeitsgerichts dürfe *„in die Privatsphäre des Arbeitnehmers nicht tiefer eingedrungen werden (...), als es der Zweck des Arbeitsverhältnisses unbedingt erfordert“*.[474] Es ist also von einer restriktiven Auslegung auszugehen und bei Vorliegen eines rechtsgeschäftlichen Schuldverhältnisses auf den Vertragszweck abzustellen ohne auf eine Zulässigkeit der Datenverwendung gemäß der in § 28 Abs. 1 Satz 1 Nr. 2 und Nr. 3 BDSG nachfolgenden Alternativen abzustellen. Der Erlaubnistatbestand des § 28 Abs. 1 Satz 1 Nr. 1 BDSG erzeugt also eine Sperrwirkung gegenüber den Erlaubnistatbeständen der Nr. 2 und Nr. 3 BDSG.[475] Die Datenverwendung im Arbeitsverhältnis kann mithin nur über die Erfüllung eigener Geschäftszwecke erlaub sein.

(ii) Erforderlichkeit

Nachdem das Vorliegen eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses bejaht worden ist, muss weiter auf den Grundsatz der Erforderlichkeit abgestellt werden. Dabei wird lediglich nach objektiven Kriterien festgestellt, ob die Daten benötigt werden, um Rechte und Pflichten aus dem Vertrag geltend machen

---

472 So *Simitis* in Simitis: Bundesdatenschutzgesetz, [8]2014, § 28, Rn. 55.
473 So *Wedde* in DKWW: Bundesdatenschutzgesetz, [4]2014, § 28, Rn. 14.
474 Bundesarbeitsgericht, Urteil vom 22.10.1986, Aktenzeichen 5 AZR 660/85, NZA 1987, S. 415-417 (416).
475 Vgl. *Plath* in Plath: BDSG, 2013, § 28, Rn. 11.

zu können.[476] Eine Interessenabwägung findet nicht statt. Es kommt also für die Prüfung der Erforderlichkeit maßgeblich auf die Zweckbestimmung des rechtsgeschäftlichen Schuldverhältnisses an. Daraus muss sich ergeben, dass von den aus dem Schuldverhältnis folgenden Rechten und Pflichten nur Gebrauch gemacht werden kann, wenn die entsprechenden Daten überhaupt verwendet werden dürfen.

Zur Datenverwendung aus vernetzten Fahrzeugen im Arbeitsverhältnis kommt es somit im Rahmen des Erlaubnistatbestandes des § 28 Abs. 1 Satz 1 Nr. 1 BDSG allein auf die Zweckbestimmung an.

Unproblematisch ist die Maßnahme erforderlich, wenn ohne die Datenverwendung die Erreichung des Geschäftszwecks absolut unmöglich ist.[477] Aber auch eine relative Unmöglichkeit soll ausreichen, um die Erforderlichkeit als gegeben zu betrachten. Dabei ist ausschlaggebend, ob die verantwortliche Stelle bei vernünftiger Betrachtung auf das in Frage stehende Mittel angewiesen ist, wobei es ausreichen soll, wenn die Wahl einer anderen Informationsmöglichkeit oder gar ein Verzicht darauf nach den Gesamtumständen nicht sinnvoll oder unzumutbar wären.[478] Insoweit müssen hier wirtschaftliche Erwägungen herangezogen werden. Es kann jedoch nicht ausreichen, wenn die Datenverwendung für die verantwortliche Stelle lediglich nützlich wäre. Eine solche Auslegung würde über den Wortlaut hinausgehen. Wie *Plath* es ausdrückt, ist der Maßstab des reinen *„nice to have"* nicht ausreichend, vielmehr müsse die Datenverwendung zumindest sinnvoll und förderlich sein, um Kosten zu vermeiden oder Prozesse zu beschleunigen.[479]

---

476 Vgl. *Taeger* in Taeger/Gabel: BDSG, [2]2013, § 28 BDSG, Rn. 47, 48; a.A. vgl. nur *Gola/Schomerus*: BDSG, [12]2015, § 28, Rn. 17., wonach zusätzlich eine Interessenabwägung vorzunehmen sein soll für die Fälle, in denen sich die Zweckbestimmung des Schuldverhältnisses nicht unmittelbar aus dem Vertragswortlaut ablesen lässt. Jedoch muss dieser Ansicht hier entgegengetreten werden. Denn es kann nicht ausschließlich auf den Vertragswortlaut abgestellt werden. Es ist vielmehr ausreichend, wenn sich der Vertragszweck aus den Umständen eindeutig feststellen lässt. Dies hat sodann anhand objektiver Kriterien zu erfolgen. Ein Abstellen allein auf den Wortlaut des Vertrages schränkt den Anwendungsbereich der Vorschrift zu sehr ein. Dies durch eine sich daran anschließende Interessenabwägung zu kompensieren, ist nicht im Sinne der Vorschrift, die eindeutig ihrem Wortlaut nach entgegen der anderen Erlaubnistatbestände in § 28 Abs. 1 Satz 1 Nr. 2 und Nr. 3 BDSG gerade nicht auf eine Interessenabwägung abstellt. Insofern ist hier allein auf objektive Kriterien abzustellen.

477 Vgl. *Plath* in Plath: BDSG, 2013, § 28, Rn. 23; dort wird z.B. die Situation genannt, dass eine Warenlieferung an einen Kunden unmöglich ist, sofern die verantwortliche Stelle die Adressdaten des Betroffenen nicht kenne.

478 So *Gola/Schomerus*: BDSG, [12]2015, § 28, Rn. 15.

479 So *Plath* in Plath: BDSG, 2013, § 28, Rn. 25.

In diesem Zusammenhang sei auch hier auf die Problematik der Erstellung von Persönlichkeitsprofilen hingewiesen. Dies betrifft im Allgemeinen Verbraucher als Kunden, deren zur Vertragsabwicklung gespeicherten Daten über sog. *„Data Mining“*[480] systematisch durchsucht und anhand dessen Kundenprofile gebildet werden.

Allerdings könnte diese Thematik zukünftig auch im vernetzten Fahrzeug technisch unter Nutzung von Big Data-Anwendungen relevant sein.[481] Es stellt sich dabei die Frage, ob eine derartige Datenverwendung noch vom Erlaubnistatbestand des § 28 Abs. 1 Satz 1 Nr. 1 BDSG gedeckt sein kann. Sollte dies verneint werden, müsste wiederum auf die soeben behandelte restriktive Auslegung der Erlaubnistatbestände des § 28 Abs. 1 Satz 1 Nr. 2 und Nr. 3 BDSG abgestellt werden. Damit die Datenverwendung durch Erstellung von Persönlichkeitsprofilen nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG erlaubt sein könnte, müsste diese für eine Phase des Beschäftigungsverhältnisses erforderlich sein, wobei zunächst auf den Vertragszweck abzustellen ist. Jedoch kann die Erstellung von Persönlichkeitsprofilen unter Anwendung von Big Data nicht mehr als vom Vertragszweck gedeckt eingeordnet werden. Das Erstellen von Persönlichkeitsprofilen dient nicht der Erfüllung des Schuldverhältnisses. Es sollen damit lediglich marketingtechnische Erkenntnisse auf Seiten der verantwortlichen Stelle erreicht werden. Da nicht schon zu Beginn der Datenerhebung feststeht, für welche Zwecke die Daten genutzt werden, kann die nachträgliche Datenverwendung zur Erstellung von Persönlichkeitsprofilen nicht gerechtfertigt sein. Denn dies ist gerade nicht als ursprüngliche Zweckbestimmung zu erkennen.

Dies gilt auch im Zusammenhang mit vernetzten Fahrzeugen und der dort möglichen Bildung von Bewegungsprofilen.

b) § 28 Abs. 1 Satz 1 Nr. 2 und Nr. 3 BDSG

Im Rahmen der Erlaubnistatbestände des § 28 Abs. 1 Satz 1 Nr. 2 und Nr. 3 BDSG kommt es auf eine Interessenabwägung zwischen den berechtigten Interessen der verantwortlichen Stelle und den schutzwürdigen Interessen des Betroffenen an. Die Abwägung der entgegenstehenden Interessen der Parteien hat nicht ausführlich[482] zu erfolgen,

---

480 Vgl. https://de.wikipedia.org/wiki/Data-Mining; dabei werden Statistiken gezielt dazu eingesetzt, aus einer Menge an Daten neue Muster zu erkennen. Die Datenberge sollen „nach wertvollem Wissen“ durchsucht werden, so die sinngemäße Übersetzung. Es geht darum, bisher nicht erkannte Zusammenhänge sichtbar zu machen.

481 Vgl. unter *Kapitel 2, Teil 5, I.* sowie *Kapitel 3, Teil 2, I.5.*.

482 So jedoch *Taeger* in Taeger/Gabel: BDSG, [2]2013, § 28 BDSG, Rn. 62.

sondern kann summarisch und am typischen Sachverhalt orientiert durchgeführt werden.[483] Die Abwägung hat unter Anwendung des Verhältnismäßigkeitsgrundsatzes zu erfolgen.[484] Es ist demnach zu prüfen, ob die Datenverwendung geeignet, erforderlich und angemessen ist. Der Bundesgerichtshof hat dies wie folgt zusammengefasst:

> *„Der wertausfüllende Begriff der ´schutzwürdigen` Belange verlangt eine Abwägung des Persönlichkeitsrechts des Betroffenen und des Stellenwerts, den die Offenlegung und Verwendung der Daten für ihn hat, gegen die Interessen der speichernden Stelle und der Dritten, für deren Zweck die Speicherung erfolgt. Dabei sind Art, Inhalt und Aussagekraft der beanstandeten Daten an den Aufgaben und Zwecken zu messen, denen ihre Speicherung dient. Nur wenn diese am Verhältnismäßigkeitsgrundsatz ausgerichtete Abwägung, die die speichernde Stelle vorzunehmen hat, keinen Grund zur Annahme bietet, dass die Speicherung der in Frage stehenden Daten zu dem damit verfolgten Zweck schutzwürdige Belange des Betroffenen beeinträchtigt, ist die Speicherung zulässig.“*[485]

Vom Überwiegen der schutzwürdigen Interessen des Betroffenen ist insbesondere auszugehen, wenn beispielsweise das Fahrverhalten des Betroffenen aufgezeichnet und in regelmäßigen Abständen an die Versicherung geschickt wird und somit je nach Aussagekraft der Daten Rückschlüsse auf das Fahrverhalten gezogen werden können.[486] In diesen Fällen ist nicht davon auszugehen, dass dies zur Wahrung berechtigter Interessen des Herstellers erforderlich ist. Die Erstellung und Nutzung eines umfassenden Persönlichkeitsprofils kann in keinem Fall unter Berufung auf berechtigte Interessen gerechtfertigt werden.[487]

Im Zweifel überwiegen jedoch die Interessen des Betroffenen mit der Folge, dass die Datenverarbeitung in diesen Fällen unzulässig ist.[488]

---

483 Vgl. *Wedde* in DKWW: Bundesdatenschutzgesetz, [4]2014, § 28, Rn. 52; *Simitis* in Simitis: Bundesdatenschutzgesetz, [8]2014, § 28, Rn. 129; *Gola/Schomerus*: BDSG, [12]2015, § 28, Rn. 28; *Plath* in Plath: BDSG, 2013, § 28, Rn. 53.

484 Bundesgerichtshof, Urteil vom 17.12.1985, Aktenzeichen VI ZR 244/84, NJW 1986, S. 2505-2507 (2506).

485 Bundesgerichtshof, Urteil vom 17.12.1985, Aktenzeichen VI ZR 244/84, NJW 1986, S. 2505-2507 (2506).

486 Vgl. *Roßnagel*, NZV 2006, S. 281–288 (284).

487 Vgl. *Roßnagel*, SVR 2014, S. 281–287 (285).

488 So *Hoeren* in Roßnagel: Handbuch Datenschutzrecht, 2003, 4.6 Zulässigkeit der Erhebung, Verarbeitung und Nutzung im privaten Bereich, Rn. 33.

c) § 32 BDSG

Ein weiterer Erlaubnistatbestand speziell für die Datenverwendung im Beschäftigungsverhältnis findet sich in § 32 BDSG[489].

Eine Verwendung personenbezogener Daten darf erfolgen, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung eines Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.[490] Vorweggenommen kann jedoch bereits an dieser Stelle festgestellt werden, dass dieser Erlaubnistatbestand lediglich eine Kosten-, Wirtschaftlichkeits- und Missbrauchskontrolle rechtfertigt und gerade nicht eine profilmäßige Aufzeichnung des Arbeitsverhaltens.[491]

(i) Das Verhältnis zwischen § 28 BDSG und § 32 BDSG

Die Anwendbarkeit des § 32 BDSG bedingt zwangsläufig eine Klarstellung, in welchem Verhältnis die verschiedenen Erlaubnistatbestände zueinander stehen. Einigkeit besteht dahingehend, dass die allgemeine Vorschrift des § 28 Abs. 1 Satz 1 Nr. 1 BDSG von der speziellen Regelung des § 32 BDSG verdrängt wird.[492] § 32 BDSG ist lex specialis zu § 28 Abs. 1 Satz 1 Nr. 1 BDSG.

Aus der Gesetzesbegründung geht explizit hervor, dass auch die Regelung des § 28 Abs. 1 S. 2 BDSG von § 32 BDSG verdrängt werden soll.[493] Dort heißt es zudem, dass sämtliche Erlaubnistatbestände des § 28 Abs. 1 BDSG keine Anwendung mehr finden sollen, wenn personenbezogenen Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden. Daraus geht der eindeutige Wille des Gesetzgebers hervor, dass die Vorschrift des § 32 BDSG die komplette Regelung des § 28 Abs. 1 BDSG verdrängen soll.

Dies gilt jedoch einschränkend nur, wenn die Daten *„für Zwecke des Beschäftigungsverhältnisses“* verwendet werden sollen. Für den Beschäftigtendatenschutz ist danach

---

489 Vgl. zum Gesetzgebungsverfahren für ein eigenes Beschäftigtendatenschutzgesetz unter *Kapitel 3, Teil 1, IV.*.

490 Vgl. § 32 Abs. 1 Satz 1 BDSG. In § 32 Abs. 1 Satz 2 BDSG ist ein Erlaubnistatbestand dafür enthalten, wann eine Datenverwendung zur Aufdeckung von Straftaten erfolgen darf.

491 Dies gilt bereits für die Datenverwendung am Arbeitsplatz selbst und muss aufgrund dessen erst Recht auch für die Arbeitnehmerkontrolle an externen Arbeitsplätzen, wie dem Dienstfahrzeug, gelten, vgl. *Schwartmann/Ohr*, RDV 2015, S. 59–68 (65).

492 So *Gola/Schomerus*: BDSG, [12]2015, § 32, Rn. 2.

493 BT-Drs. 16/13657 vom 01.07.2009, S. 20, http://dipbt.bundestag.de/dip21/btd/16/136/1613657.pdf.

ausschließlich § 32 BDSG anzuwenden. Etwas anderes gilt lediglich für die Datenverwendung zwar innerhalb des Beschäftigungsverhältnisses, jedoch zu anderen Zwecken. Für andere Zwecke können also auch im Verhältnis zwischen Arbeitgeber und Beschäftigten die Erlaubnistatbestände des § 28 Abs. 1 Satz 1 Nr. 2 und Nr. 3 BDSG Anwendung finden.[494]

Dieses Ergebnis kann neben der Wortlautauslegung auch durch grammatikalische Auslegung untermauert werden. Denn während § 28 BDSG ausweislich seiner Überschrift für die Datenerhebung und -speicherung zu – sämtlichen – eigenen Geschäftszwecken Anwendung findet, ist die Vorschrift des § 32 BDSG auf die Datenerhebung, -verarbeitung und –nutzung für Zwecke des Beschäftigungsverhältnisses reduziert. Einzig der Erlaubnistatbestand des § 28 Abs. 1 Satz 1 Nr. 1 BDSG nimmt Bezug auf das Vorliegen eines rechtsgeschäftlichen Schuldverhältnisses. Der Anwendungsbereich des § 28 BDSG muss hier hinter § 32 BDSG zurücktreten.

Auch Sinn und Zweck der Vorschrift des § 32 BDSG sprechen hier dafür, die gesamte Regelung des § 28 Abs. 1 BDSG nicht mehr neben § 32 BDSG anzuwenden, sofern es sich um eine Datenverwendung zu Beschäftigungszwecken handelt. Denn ansonsten könnte neben dem Vertragszweck auch eine allgemeine Abwägung dazu herangezogen werden, eine Datenverwendung zu erlauben. Dies würde den Arbeitgeber bevorteilen, weil das Gewicht zugunsten des Informationsinteresses des Arbeitgebers verschoben wäre.[495]

Die Erlaubnistatbestände der § 28 Abs. 1 Satz 1 Nr. 2 und Nr. 3 BDSG werden nur dann nicht von § 32 BDSG verdrängt, soweit die Datenverwendung *„andere Zwecken“*, also *„beschäftigungsfremde“*[496] Zwecken betrifft.

Im Rahmen der Prüfung der Rechtmäßigkeit einer Datenverwendung aus vernetzten Fahrzeugen ist somit der Zweck maßgeblich zu bestimmen und herauszuarbeiten, ob es sich dabei noch um Beschäftigungszwecke handelt.

(ii) Zweckbestimmung

Die Zweckbestimmung des § 32 Abs. 1 Satz 1 BDSG orientiert sich an den verschiedenen zeitlichen Phasen, die im Zusammenhang mit einem Beschäftigungsverhältnis ste-

494 BT-Drs. 16/13657 vom 01.07.2009, S. 21, http://dipbt.bundestag.de/dip21/btd/16/136/1613657.pdf.
495 Vgl. *Däubler* in DKWW: Bundesdatenschutzgesetz, [4]2014, § 32, Rn. 8a.
496 So *Erfurth*, NJOZ 2009, S. 2914–2927 (2922).

hen. Umfasst sind alle Datenverwendungen, die für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich sind. Wie auch bereits im Rahmen des Erlaubnistatbestandes nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist hier an das auslegungsbedürftige Tatbestandsmerkmal der Erforderlichkeit anzuknüpfen. In der Gesetzesbegründung zu § 32 Abs. 1 Satz 1 BDSG heißt es dazu, dass die Regelung auch insoweit den bisher von der Rechtsprechung erarbeiteten allgemeinen Grundsätzen des Datenschutzes im Beschäftigungsverhältnis entspreche.[497] Für das Vorliegen der Erforderlichkeit bedeutet dies nach der Rechtsprechung, dass ein unmittelbarer Zusammenhang zwischen der beabsichtigten Datenverwendung und dem konkreten Vertragszweck bestehen muss.[498] Es darf *„in die Privatsphäre des Arbeitnehmers nicht tiefer eingedrungen werden (...), als es der Zweck des Arbeitsverhältnisses unbedingt erfordert"*.[499]

Für diese Feststellung ist auf eine Interessenabwägung nach den Grundsätzen der Verhältnismäßigkeit abzustellen.[500] Die Datenverwendung muss danach geeignet, erforderlich und angemessen sein, um den erstrebten Zweck zu erreichen.[501] Dabei kommt es maßgeblich auf den bereits zuvor festgelegten Zweck der Datenverwendung an. Die Datenverwendung ist geeignet, wenn mit ihrer Hilfe der erstrebte Zweck gefördert werden kann.[502] Nach der Rechtsprechung des Bundesverfassungsgerichts verlangt das Gebot der Verhältnismäßigkeit im engeren Sinn, *„dass die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe stehen darf"*.[503] Die gegenseitigen betroffenen Interessen sind somit gegeneinander abzuwägen. Um diesbezüglich eine Feststellung zu treffen, bedarf es einer Ge-

---

497 BT-Drs. 16/13657 vom 01.07.2009, S. 21, http://dipbt.bundestag.de/dip21/btd/16/136/1613657.pdf unter Bezugnahme auf die Rechtsprechung des Bundesarbeitsgerichts (Urteil vom 22.10.1986, Aktenzeichen 5 AZR 660/85, NZA 1987, S. 415-417 und Urteil vom 07.09.1995, Aktenzeichen 8 AZR 828/93, NZA 1996, S. 637-640.

498 Vgl. *Zöll* in Taeger/Gabel: BDSG, [2]2013, § 32 BDSG, Rn. 17.

499 Bundesarbeitsgericht, Urteil vom 22.10.1986, Aktenzeichen 5 AZR 660/85, NZA 1987, S. 415-417 (416).

500 Bundesarbeitsgericht, Urteil vom 22.10.1986, Aktenzeichen 5 AZR 660/85, NZA 1987, S. 415-417 (415); Bundesarbeitsgericht, Beschluss vom 11.03.1986, Aktenzeichen 1 ABR 12/84, NZA 1986, S. 526-530 (528); Bundesarbeitsgericht, Beschluss vom 26.08.2008, Aktenzeichen 1 ABR 16/07, NZA 2008, S. 1187-1194 (1187).

501 Vgl. *Di Fabio* in Maunz/Dürig: Grundgesetz, [72. EL]2014, Art. 2, Rn. 41.

502 Bundesarbeitsgericht, Beschluss vom 26.08.2008, Aktenzeichen 1 ABR 16/07, NZA 2008, S. 1187-1194 (1190)

503 Bundesverfassungsgericht, Beschluss vom 04.04.2006, Aktenzeichen 1 BvR 518/02, NJW 2006, S. 1939-1951 (1941).

samtabwägung der Intensität des Eingriffs und des Gewichts der ihn rechtfertigenden Gründe.[504]

Es ist im Rahmen der Erforderlichkeit nach § 32 BDSG mithin immer zu fragen, ob die verantwortliche Stelle das gleiche Ziel auch mit einem geringeren Eingriff in das Recht auf informationelle Selbstbestimmung des Betroffenen erreichen kann.[505] Dabei ist auch zu berücksichtigen, ob ein etwaiger Verzicht auf die Datenverwendung möglich ist.[506]

Es sind alle Daten für eine Phase des Beschäftigungsverhältnisses im Sinne des § 32 Abs. 1 Satz 1 BDSG bestimmt, die der Arbeitgeber zur Erfüllung seiner Pflichten sowie zur Wahrnehmung seiner Rechte gegenüber dem Arbeitnehmer vernünftigerweise benötigt. Im Rahmen der Erforderlichkeit kommt es für den Erlaubnistatbestand des § 32 Abs. 1 Satz 1 BDSG darauf an, dass die Datenverwendung dem Beschäftigungsverhältnis dient und dafür nicht nur nützlich ist.[507] Etwas anderes gilt nur, wenn von mehreren gleichermaßen wirksamen Maßnahmen, die den Arbeitnehmer stärker belastende gewählt wurde, wobei insoweit auch das Gebot der Datensparsamkeit nach § 3a BDSG greift.[508] Eine absolute Notwendigkeit für die Datenverwendung muss nicht gegeben sein, denn es ist ausreichend, wenn die berechtigten Interessen nicht auf andere Weise angemessen gewahrt werden können.[509] Insoweit kann auf die bereits zu § 28 BDSG aufgestellten Grundsätze zurückgegriffen werden.[510]

2. Die Erlaubnis zur Datenverwendung durch *"eine andere Rechtsvorschrift"*

Für die Datenverwendung aus vernetzten Fahrzeugen ist der Erlaubnistatbestand der Datenverwendung *„durch eine andere Rechtsvorschrift“* von erheblicher Bedeutung.

Neben den im Bundesdatenschutzgesetz geregelten ausdrücklichen Erlaubnistatbeständen können solche auch in *„anderen Rechtsvorschriften“* enthalten sein. Damit eine Rechtsvorschrift geeignet ist, als Erlaubnis für eine Datenverwendung zu dienen, muss sich aus ihr – zumindest durch Auslegung – ergeben, welche Stelle unter welchen Voraussetzungen zu welchen Zwecken personenbezogene Daten in welcher Weise erheben

---

504 Bundesarbeitsgericht, Beschluss vom 26.08.2008, Aktenzeichen 1 ABR 16/07, NZA 2008, S. 1187-1194.
505 Vgl. *Thüsing*, NZA 2009, S. 865–870 (867).
506 Vgl. *Zöll* in Taeger/Gabel: BDSG, [2]2013, § 32 BDSG, Rn. 18.
507 So *Däubler*, NZA 2001, S. 874–881 (876).
508 Vgl. *Gola/Schomerus*: BDSG, [12]2015, § 32, Rn. 10.
509 Vgl. *Gola/Klug*: Grundzüge des Datenschutzrechts, 2003, S. 91.
510 Vgl. unter *Kapitel 3, Teil 3, I.1.a)(ii).*

darf.[511] Die Verwendung der Daten muss in der jeweiligen Rechtsvorschrift angeordnet oder erlaubt werden.

a) Betriebsvereinbarungen

Für die hier relevante Datenverwendung im Rahmen eines Beschäftigungsverhältnisses ist anerkannt[512], dass auch Betriebsvereinbarungen als *„andere Rechtsvorschrift“* im Sinne des § 4 Abs. 1 BDSG[513] herangezogen und als Erlaubnistatbestand Geltung beanspruchen können. Begründet wird dies damit, dass die Verarbeitung von Personaldaten im Betrieb sinnvoll nur nach einheitlichen Gesichtspunkten erfolgen könne.[514] Zudem können durch entsprechende Gestaltung von Betriebsvereinbarungen auch Unsicherheiten bezüglich einer Widerrufbarkeit oder einer etwaig fehlenden Freiwilligkeit der Einwilligung vermieden werden.[515] Auch der Aspekt einer Vertrauensgarantie seitens des Arbeitgebers spielt dabei eine Rolle. Denn der Arbeitgeber, der eine den Datenschutz des Beschäftigten konkretisierende oder verbessernde Betriebsvereinbarung zur Grundlage der Nutzung betrieblicher Kommunikationsmittel und der diesbezüglichen Kontrollmaßnahmen macht, gibt gleichzeitig gegenüber dem Beschäftigten eine Vertrauensgarantie dahingehend ab, dass darüber hinausgehende Eingriffe in deren Persönlichkeitsrecht nicht erfolgen.[516]

Es können nach Ansicht des Bundesarbeitsgerichts auch solche Betriebsvereinbarungen als Erlaubnistatbestand herangezogen werden, die Regelungen zu Datenverwendungen enthalten, welche von dem Mindeststandard des Bundesdatenschutzgesetzes abwei-

---

511 Vgl. *Bäcker* in Wolff/Brink: Datenschutzrecht in Bund und Ländern, 2013, § 4, Rn. 5.

512 Bundesarbeitsgericht, Beschluss vom 27.05.1986, Aktenzeichen 1 ABR 48/84, NZA 1986, S. 643-650 (646); Bundesarbeitsgericht, Beschluss vom 30.08.1995, Aktenzeichen 1 ABR 4/95, NZA 1996, S. 218-222 (221); Bundesarbeitsgericht, Beschluss vom 20.12.1995, Aktenzeichen 7 ABR 8/95, NZA 1996, S. 945-948 (947).

513 Im Rahmen der Novellierung des nationalen Beschäftigtendatenschutzes ist außerdem vorgesehen, eine Klarstellung mit aufzunehmen, wonach Betriebs- und Dienstvereinbarungen als *„andere Rechtsvorschriften im Sinne dieses Gesetzes“* einzuordnen sind, vgl. dazu § 4 Abs. 1 BDSG-E: *„Andere Rechtsvorschriften im Sinne dieses Gesetzes sind auch Betriebs- und Dienstvereinbarungen.“*.

514 Vgl. *Gola/Schomerus*: BDSG, [12]2015, § 4, Rn. 10.

515 So *Freckmann/Störing/Müller*, BB 2011, S. 2549 (2549).

516 Vgl. *Gola*: Datenschutz am Arbeitsplatz, [5]2014, Rn. 523.

chen.[517] Jedoch ist zu beachten, dass die Betriebsvereinbarungen zwar über das Schutzniveau des Bundesdatenschutzgesetzes hinausgehen dürfen, aber auch diese Befugnis nicht uneingeschränkt Geltung beanspruchen kann. Das Bundesarbeitsgericht hat in seiner Entscheidung vom 27.05.1986 festgestellt, dass die sich aus *„grundgesetzlichen Wertungen, zwingendem Gesetzesrecht und den allgemeinen Grundsätzen des Arbeitsrechts ergebenden Beschränkungen“* zu beachten sind.[518] Der Regelungsspielraum ist zudem begrenzt durch die Achtung der Persönlichkeitsrechte der Arbeitnehmer sowie durch die Regelungen des Unionsrechts.[519] Diese Einschränkungen sollten auch im gestoppten Entwurf des Bundesdatenschutzgesetzes Berücksichtigung finden.[520]

Das Bundesarbeitsgericht begründet seine Entscheidung mit dem im Arbeitsrecht geltenden Günstigkeitsprinzip. Danach können niederrangige Vorschriften, wie z.B. Betriebsvereinbarungen, den höherrangigen Vorschriften vorgehen, jedoch nur in dem Maße, in dem sie für den Arbeitnehmer günstiger sind.[521]

Der notwendige normative Charakter von Betriebsvereinbarungen folgt aus § 77 Abs. 4 Satz 1 BetrVG.[522] Sie gelten danach unmittelbar und zwingend. Durch Betriebsvereinbarungen sind somit auch Verschlechterungen für die Position des Betroffenen denkbar. Das Bundesarbeitsgericht löst diesen Konflikt, indem es solche nicht mit dem Bundesdatenschutzgesetz zu vereinbarende Klauseln in Betriebsvereinbarungen an dem Verhältnismäßigkeitsgrundsatz misst. Insgesamt ist also eine Unterschreitung des Schutzniveaus des Bundesdatenschutzgesetzes im Rahmen von Betriebsvereinbarungen möglich,

---

517 Vgl. a.A. nur *Sokol*, nach welchem Betriebsvereinbarungen gerade nicht hinter dem Schutzniveau des Bundesdatenschutzgesetzes zurückbleiben dürfen, vgl. *Scholz/Sokol* in Simitis: Bundesdatenschutzgesetz, [8]2014, § 4, Rn. 17. Allerdings muss dabei zwangsläufig die Frage gestellt werden, aus welchem Grund in diesen Fällen überhaupt andere als die im Bundesdatenschutzgesetz selbst geregelten Erlaubnistatbestände hätten geschaffen werden müssen. Insoweit würde es keinen Sinn machen, auch andere Rechtsvorschriften ebenfalls in die Regelung des § 4 Abs. 1 BDSG mit aufzunehmen. Zudem würden dadurch die Befugnisse der Betriebsparteien derart eingeschränkt, dass sie von ihrem Recht keinen hinreichenden Gebrauch mehr machen könnten. Dies kann nicht im Sinne der Vorschrift sein.

518 Bundesarbeitsgericht, Beschluss vom 27.05.1986, Aktenzeichen 1 ABR 48/84, NZA 1986, S. 643 (647).

519 Vgl. *Bäcker* in Wolff/Brink: Datenschutzrecht in Bund und Ländern, 2013, § 4, Rn. 15.

520 In einem Änderungsvorschlag des Bundesrates heißt es zu § 32l BDSG-E: *„Soweit in Tarifverträgen und Dienstvereinbarungen von den übrigen Vorschriften dieses Unterabschnitts abgewichen wird, haben diese die sich aus grundgesetzlichen Wertungen und den allgemeinen Grundsätzen des Arbeitsrechts ergebenden Beschränkungen zu beachten und der datenschutzrechtlichen Verantwortung Rechnung zu tragen“*, vgl. BR-Drs. 535/2/10 vom 25.10.2010, S. 43, http://dipbt.bundestag.de/dip21/brd/2010/0535-2-10.pdf.

521 Vgl. https://de.wikipedia.org/wiki/Günstigkeitsprinzip.

522 Vgl. *Gola/Schomerus*: BDSG, [12]2015, § 4, Rn. 10.

soweit die Grundsätze informationeller Selbstbestimmung eingehalten werden, die das Bundesverfassungsgericht im Volkszählungsurteil aufstellte.[523]

Der erste Senat des Bundesarbeitsgerichts hat in einer neueren Entscheidung[524] zur Wirksamkeit einer Compliance-Betriebsvereinbarung die Anforderungen an den Umgang mit Beschäftigtendaten durch Betriebsvereinbarungen präzisiert. Zunächst stellte das Bundesarbeitsgericht fest, dass es auch weiterhin an seiner Rechtsprechung festhalte, wonach Betriebsvereinbarungen auch zuungunsten des Arbeitnehmers dessen allgemeines Persönlichkeitsrecht einschränken können und dies an dem Grundsatz der Verhältnismäßigkeit zu messen sei.[525] Dadurch soll ein Ausgleich zwischen den Interessen des Arbeitsgebers und den von ihm verfolgten Zwecken sowie den Interessen des Arbeitnehmers und dem durch die Maßnahme erfolgenden Eingriff in seine Persönlichkeitsrechte hergestellt werden. Mithin kommt den betroffenen Grundrechten der Beschäftigten im Rahmen der Auslegung des § 32 Abs. 1 BDSG sowie des § 75 Abs. 2 BetrVG eine mittelbare Drittwirkung zu.[526] Der Schwerpunkt der Prüfung liegt im Rahmen der Entscheidung des Bundesarbeitsgerichts bei der Angemessenheit. Für die dabei festzustellende Zweck-Mittel-Relation kommt es auf die Tiefe des jeweiligen Eingriffs ebenso an wie auf die Streubreite der Maßnahmen mit der Folge, dass stichprobenartige oder anlassbezogene Kontrollen weniger belastend sind als flächendeckende oder anlassunabhängige Kontrollen.[527] Da auch im Rahmen des Erlaubnistatbestandes des § 32 Abs. 1 Satz 2 BDSG eine Abwägung vorzunehmen ist, ob die Maßnahme erforderlich ist und ob die schutzwürdigen Interessen des Arbeitnehmers überwiegen, wird die gegenständliche Entscheidung des Bundesarbeitsgerichts wohl auch die Anwendung und Auslegung des § 32 BDSG beeinflussen.

An den soeben dargestellten Grundsätzen ändert sich allerdings auch nach Erlass der Datenschutz-Grundverordnung nichts. Zum jetzigen Zeitpunkt fehlt ein Erlaubnistatbestand, der die Datenverwendung aufgrund von Betriebs- oder Dienstvereinbarungen zulassen würde. Lediglich im Rahmen der Öffnungsklausel des Art. 88 DS-GVO ist für die Mitgliedsstaaten eine Ermächtigung vorgesehen, per Gesetz die Verarbeitung von

---

523 So auch *Kirsch*, MMR-aktuell 2011, 317362.

524 Bundesarbeitsgericht, Vorlagebeschluss vom 09.07.2013, Aktenzeichen 1 ABR 2/13 (A), NZA 2013, S. 1433-1438.

525 Bundesarbeitsgericht, Vorlagebeschluss vom 09.07.2013, Aktenzeichen 1 ABR 2/13 (A), NZA 2013, S. 1433-1438 (1435).

526 So *Wybitul*, NZA 2014, S. 225-232 (227).

527 So *Wybitul*, NZA 2014, S. 225-232 (229).

personenbezogenen Daten mit Beschäftigungskontext zu regeln. Darunter fällt auch die Verabschiedung von Betriebsvereinbarungen.[528] Dies stellte jedoch keine Ermächtigungsgrundlage dar. In der maßgeblichen Vorschrift des Art. 6 DS-GVO zur Rechtmäßigkeit der Verarbeitung, die auch die Erlaubnistatbestände enthält, fehlt jeglicher Bezug zu Betriebs- oder Dienstvereinbarungen. Dies unterscheidet sich insoweit wesentlich von der nationalen Regelung des § 4 Abs. 1 BDSG.

Diese Problematik wurde bisher auch nicht auf europäischer Ebene diskutiert.[529] Es ist hier jedoch durch die Formulierung *„in den Grenzen der Verordnung“* und nach allgemeinen Grundsätzen[530] von einer engen Auslegung der Öffnungsklausel als Ausnahme von gemeinschaftsrechtlichen Grundsätzen auszugehen, sodass insoweit noch kritisch zu hinterfragen ist, ob trotz alledem durch den nationalen Gesetzgeber eine Delegation der Befugnisse an die Verantwortlichen zur Schaffung von Betriebsvereinbarungen möglich sein soll.

Es gibt insoweit bereits Stimmen, die die Vorschriften der Datenschutz-Grundverordnung derart günstig auslegen wollen, dass spezielle Regelungen in Kollektivvereinbarungen auch auf europäischer Ebene möglich sein sollen.[531] Dem nationalen Gesetzgeber soll eine Regelung zur Problematik möglich sein, inwieweit Betriebsvereinbarungen als Erlaubnistatbestand herangezogen werden können. Es bleibt jedoch die hierzu ergehende Rechtsprechung abzuwarten.

b) Die Vorschriften des IVSG

Als *„andere Rechtsvorschrift“* im Sinne des § 4 Abs. 1 BDSG kommen im Zusammenhang mit vernetzten Kraftfahrzeugen allerdings auch die Vorschriften des Intelligente

---

528 Vgl. Erwägungsgrund (155) DS-GVO, wonach in Kollektivvereinbarungen (einschließlich 'Betriebsvereinbarungen') spezifische Vorschriften für die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorgesehen werden können; vgl. auch *Forst*, ZD 2012, S. 251–255 (252).

529 Vgl. *Stellungnahme zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) vom 04.03.2013*, vorgelegt von Nadja Hirsch (MdEP), COM (2012)0011 - C7-0025/2012 - 2012/0011(COD), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-498.045+02+DOC+PDF+V0//DE&language=DE; darin wird lediglich erwähnt, dass eine Festlegung von für den Arbeitnehmer günstigen Standards auch in kollektiven Vereinbarungen möglich sein muss, vgl. aaO, S. 3.

530 Bundesgerichtshof, Beschluss vom 19.01.2010, Aktenzeichen StB 27/09, NJOZ 2010, S. 1274-1290 (1282); Europäischer Gerichtshof, Urteil vom 15.12.1976, Aktenzeichen Rs. 41/76, NJW 1977, S. 1007-1008 (1008).

531 So *Forst*, NZA 2012, S. 364–367 (366).

Verkehrssysteme Gesetzes[532] in Betracht, dort insbesondere § 3 Satz 2 IVSG. Grundsätzlich ist der Anwendungsbereich des Intelligente Verkehrssysteme Gesetzes als weit einzustufen. Das Intelligente Verkehrssysteme Gesetz gilt für Intelligente Verkehrssysteme im Straßenverkehr und deren Schnittstellen zu anderen Verkehrsträgern.[533]

Insgesamt ist der Anwendungsbereich des Intelligente Verkehrssysteme Gesetzes relativ abstrakt. Dies begründet sich damit, dass das Intelligente Verkehrssysteme Gesetz eine Ermächtigung zum Erlass von Rechtsverordnungen enthält[534], von welcher bisher jedoch noch kein Gebrauch gemacht wurde. Zudem muss bei der Einführung von Diensten und Anwendungen nach dem Intelligente Verkehrssysteme Gesetz darauf geachtet werden, dass die von der EU-Kommission aufgrund von Art. 6 IVS-RL erlassenen Spezifikationen eingehalten werden.

In den Anwendungsbereich des Gesetzes fallen aber in jedem Fall Intelligente Verkehrssysteme wie individuelle Navigationsgeräte, sog. kollektive Verkehrsbeeinflussungsanlagen auf Autobahnen[535], die Verkehrsdatenerfassung oder Informationsdienste für LKW-Parken sowie die Fernschaltung von Ampelanlagen. Die Einführung intelligenter Verkehrssysteme dient mithin vorwiegend der Verbindung zwischen Fahrzeug und Infrastruktur, wie dies auch § 4 Nr. 4 IVSG klarstellt.

Es stellt sich allerdings die Frage, welche Bedeutung das Intelligente Verkehrssysteme Gesetz für den Datenschutz haben kann. Denn im Rahmen des dortigen Erlaubnistatbestandes des § 3 Satz 2 IVSG heißt es:

> *„Personenbezogene Daten dürfen nur erhoben, verarbeitet oder genutzt werden, soweit dies durch eine bundesgesetzliche Regelung ausdrücklich zugelassen oder angeordnet wird."*

---

532 Die Veröffentlichung im Bundesgesetzblatt erfolgte am 20.06.2013, vgl. BGBl. I 2013, Nr. 29 vom 20.06.2013, S. 1553; vgl. unter *Kapitel 3, Teil 1, VI.*.

533 Als Intelligente Verkehrssysteme bezeichnet das Gesetz Systeme, bei denen Informations- und Kommunikationstechnologien im Straßenverkehr und an Schnittstellen zu anderen Verkehrsträgern eingesetzt werden. Unter *„Anwendungen Intelligenter Verkehrssysteme"* sind schließlich technische Systeme, Verfahren oder Geräte für den Einsatz intelligenter Verkehrssysteme zu verstehen. Die Bereitstellung solcher Anwendungen wird als *„Dienst Intelligenter Verkehrssysteme"* bezeichnet, hierzu insgesamt §§ 1 Satz 1, 2 Nr. 1-3 IVSG.

534 Vgl. § 5 IVSG.

535 Vgl. dazu *Daduna/Voß*: Informationsmanagement im Verkehr, 2000, S. 215.

Im Gegensatz dazu steht die Regelung des § 4 Abs. 1 BDSG:

> *„Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat."*

Während also nach dem Bundesdatenschutzgesetz auch eine Einwilligung des Betroffenen für die Zulässigkeit der Datenverwendung ausreicht, kann im Rahmen des Intelligente Verkehrssysteme Gesetz nur auf eine bundesgesetzliche Regelung abgestellt werden, die dies ausdrücklich zulässt oder anordnet. Es stellt sich somit die Frage, wie diese beiden Regelungen wirken und wie insoweit die Vorschrift des § 3 Satz 2 IVSG auszulegen sein wird.

Man könnte zum einen den Standpunkt vertreten, es handele sich bei der Vorschrift des § 3 Satz 2 IVSG um eine Spezialvorschrift, die als lex specialis zu § 4 Abs. 1 BDSG diesem vorginge. Für diesen Fall wäre eine Einwilligung in die Datenverwendung im Rahmen intelligenter Verkehrssysteme nicht möglich. Die spezielle Vorschrift würde der allgemeinen Regelung vorgehen, sodass ein Rückgriff auf die allgemeine Vorschrift des § 4 Abs. 1 BDSG nicht gestattet wäre.

Andererseits könnte aber auch die Auffassung vertreten werden, § 3 Satz 2 IVSG sei rein deklaratorisch. Dies hätte zur Folge, dass es weiterhin bei der Geltung des § 4 Abs. 1 BDSG bliebe.

Es könnte auch davon ausgegangen werden, dass es sich bei der Regelung des § 3 Satz 2 IVSG insoweit um ein redaktionelles Versehen handelt, als dass der Ausschluss der Einwilligungsmöglichkeit gesetzgeberisch nicht gewollt war.

Es kann festgestellt werden, dass der in § 3 Satz 2 IVSG geregelte Erlaubnistatbestand in datenschutzrechtlicher Hinsicht unglücklich formuliert ist. Die Vorschrift des § 3 Satz 2 dient der Umsetzung des Art. 10 IVS-RL. Dort wird jedoch gerade in Art. 10 Abs. 4 IVS-RL vorgeschrieben, dass die Bestimmungen der Datenschutz-Richtlinie über die Einwilligung in die Verarbeitung personenbezogener Daten eingehalten werden. Schon daraus ergibt sich, dass der Wortlaut des § 3 Satz 2 IVSG keinesfalls dahingehend zu verstehen ist, eine Einwilligung in die Datenverwendung sei im Anwendungsbereich des Intelligente Verkehrssysteme Gesetzes nicht gestattet. Noch dazu schreibt Art. 10 Abs. 1 IVS-RL vor, dass von den Mitgliedsstaaten die Bestimmungen

der Datenschutz-Richtlinie einzuhalten sind. Da die Datenschutz-Richtlinie nach der Rechtsprechung des Europäischen Gerichtshofs[536] zu einer *„umfassenden Harmonisierung“* führt, muss § 3 Satz 2 IVSG dahingehend ausgelegt werden, dass durch diese Vorschrift nicht die Möglichkeit ausgeschlossen wird, auf den Erlaubnistatbestand der Einwilligung zurückzugreifen.

Zum jetzigen Zeitpunkt lässt sich insoweit noch keine abschließende Beurteilung dieser Streitfrage treffen. Denn bislang wurde von der Rechtsverordnungsermächtigung kein Gebrauch gemacht. Sobald jedoch die ersten Durchführungsverordnungen gelten, dürfte dieser Aspekt an Relevanz gewinnen. Dies ist insbesondere auch aufgrund der rasant fortschreitenden technischen Entwicklung der intelligenten Verkehrssysteme notwendig.

II. Die Einwilligung als Erlaubnistatbestand

Für den Fall, dass eine Datenverwendung nicht bereits durch eine Rechtsvorschrift zulässig ist, kann dies auch aufgrund der Einwilligung des Betroffenen erlaubt sein. Auch dieses Instrument spielt für die Datenverwendung im Arbeitsverhältnis eine herausragende Bedeutung.

1. Grundsätzliches

Die Möglichkeit zur Erteilung einer Einwilligung ist seitens des Betroffenen genuiner Ausdruck des Rechts auf informationelle Selbstbestimmung und macht deutlich, dass der Betroffene selbst darüber entscheiden kann, *„was mit seinen personenbezogenen Daten passiert und wer was wann über ihn weiß“*.[537] Da der Betroffene in Gestalt der Einwilligung eine *„Bestimmung“* über seine Daten dahingehend trifft, dass er die Daten preisgibt oder einer Datenverwendung zustimmt, ist dies als Ausübung des Rechts auf informationelle Selbstbestimmung und damit als Grundrechtsausübung zu sehen.[538]

---

536 Europäischer Gerichtshof, Urteil vom 06.11.2003, Aktenzeichen C-101/01, EuZW 2004, S. 245-252 (251).

537 So *Kühling* in Wolff/Brink: Datenschutzrecht in Bund und Ländern, 2013, § 4a, Rn. 1.

538 So *Geiger*, NVwZ 1989, S. 35-38 (37).; a.A. vgl. nur *Robbers*, JuS 1985, S. 925-931 (928).

Die Anforderungen, die an die Wirksamkeit einer Einwilligung gestellt werden, sind in § 4a BDSG[539] geregelt. Danach muss die Einwilligung auf der freien Entscheidung des Betroffenen beruhen.[540] Dies kann vor allem im Anwendungsbereich von Arbeitsverhältnissen problematisch werden.

a) Rechtsnatur

Die Rechtsnatur der Einwilligung ist umstritten, wobei im Rahmen der vorliegenden Untersuchung davon ausgegangen wird, dass es sich um eine Willenserklärung mit rechtsgeschäftlichem Charakter handelt und gerade nicht um einen reinen Realakt.[541] Entsprechend der Terminologie des § 183 BGB handelt es sich bei der Einwilligung nach der Legaldefinition um eine vorherige Zustimmung, wodurch bereits klargestellt wird, dass die Einwilligung zeitlich vor der Datenverwendung eingeholt werden muss. Eine erst nach der Datenverwendung erklärte Einwilligung ist in Form der Genehmigung nach der Terminologie des § 184 BGB nicht ausreichend. Letzteres wird allerdings als Einwilligung in die zukünftige Verwendung gesehen und beseitigt damit die Löschungspflicht der verantwortlichen Stelle.[542] Ausgeschlossen ist es allerdings, eine erteilte, aber unwirksame Einwilligung im Nachhinein nachträglich heilen zu wollen.[543]

---

539 Auf die Einwilligungsmöglichkeit im Bereich der Werbung und des Adresshandels durch nichtöffentliche Stellen nach § 28 Abs. 3 Satz 1, Abs. 3a BDSG soll hier nicht näher eingegangen werden. Im Bereich des Telemediengesetzes sind die Vorschriften der §§ 11 Abs. 2, 12 Abs. 2 TMG vorrangig, soweit es sich um personenbezogene Daten handelt, die der Bereitstellung von Telemediendiensten dienen, vgl. *Plath* in Plath: BDSG, 2013, § 4a, Rn. 69.

540 Erforderlich für eine wirksame Einwilligung ist zusätzlich ein Hinweis auf den vorgesehenen Zweck der Datenverwendung sowie – soweit erforderlich oder vom Betroffenen verlangt – ein Hinweis auf die Folgen der Verweigerung der Einwilligung. Durch Letzteres wird zweckmäßig verhindert, dass dem Betroffenen im Falle der Verweigerung seiner Einwilligung ein Nachteil daraus entsteht. Soweit nicht wegen besonderer Umstände eine andere Form angemessen ist, muss die Einwilligung der Schriftform genügen. Die Einwilligung ist besonders hervorzuheben, wenn sie zusammen mit anderen Erklärungen schriftlich erteilt wird. Bei der Verwendung besonderer Arten personenbezogener Daten ist die Einwilligung ausdrücklich auch auf diese Daten zu beziehen, vgl. hierzu insgesamt §§ 4a Abs. 1 Satz 1, Satz 2, Satz 3, Satz 4 und Abs. 3 BDSG.

541 So *Simitis* in Simitis: Bundesdatenschutzgesetz, [8]2014, § 4a, Rn. 20; *Gola/Schomerus*: BDSG, [12]2015, § 4a, Rn. 2; a.A. vgl. *Däubler* in DKWW: Bundesdatenschutzgesetz, [4]2014, § 4a, Rn. 5; der hier vertretenen Auffassung ist jedoch mit der Argumentation zu folgen, dass es sich bei dem Begriff der „*Einwilligung*“ um eine der Terminologie des Bürgerlichen Gesetzbuches entsprechende Anwendung handelt. Im Rahmen des § 183 BGB wird die Einwilligung legaldefiniert als vorherige Zustimmung. Dabei wird ebenfalls davon ausgegangen, dass es sich um eine Willenserklärung und nicht um einen bloßen Realakt handelt. Der Streit wird vorwiegend im Zusammenhang mit der Frage relevant, welche Anforderungen an eine wirksame Einwilligung Minderjähriger zu stellen sind. Dies soll jedoch für die vorliegende Untersuchung nicht weiter von Relevanz sein.

542 Vgl. *Plath* in Plath: BDSG, 2013, § 4a, Rn. 81.

543 Vgl. *Tinnefeld/Buchner/Petri*: Einführung in das Datenschutzrecht, [5]2012, S. 341.

b) Freie und informierte Erklärung

Besonders problematisch erscheint im Zusammenhang mit vernetzten Fahrzeugen und der daraus oft für den Betroffenen nicht erkennbaren und unwissentlich erfolgenden Datenverwendung sowie auch in Bezug auf die Datenverwendung in Arbeitsverhältnissen die Voraussetzung der freien und informierten Erklärung, um von einer ordnungsgemäß erteilten Einwilligung ausgehen zu können.

Bei der Einwilligung muss es sich in jedem Fall um eine freie und informierte Erklärung handeln. Als freie Entscheidung ist eine Einwilligung nur einzustufen, wenn diese zwanglos erfolgt. Die Wirksamkeit der Einwilligung setzt insoweit voraus, dass der Betroffene *„in Kenntnis der Sachlage“* die Einwilligung erteilt.[544] Der Betroffenen kann mithin eine tatbestandsmäßig informierte Entscheidung nur treffen, wenn er auf den vorgesehen Zweck der Datenverwendung sowie unter Umständen auf die Folgen einer Verweigerung der Einwilligung hingewiesen wurde. Erst dadurch kann er sich der Reichweite seiner Einwilligung bewusst sein. Der Betroffene ist über die Identität der verantwortlichen Stelle, die Zweckbestimmung der Datenverwendung und die Kategorien von Empfängern zu unterrichten.[545] Dies sind Anhaltspunkte, an denen sich ein Hinweis nach § 4a Abs. 1 Satz 2 BDSG orientieren kann.

Inhaltlich muss sich die Einwilligung nach Bestimmtheitsgrundsätzen auf den jeweiligen Einzelfall beziehen. Dies ergibt sich bereits aus der Regelung des § 4 Abs. 1 BDSG, wonach die Datenverwendung nur zulässig ist, *„soweit“* der Betroffenen eingewilligt hat. Der Grad der Bestimmtheit der Einwilligungserklärung ist abhängig von der konkreten Datenverwendung, steigt jedoch umso mehr an, je mehr Persönlichkeitsschutz betroffen ist.[546]

Die Einwilligung erfolgt in den meisten Fällen in formularmäßiger Form. Es werden meist vorformulierte Vertragsbedingungen gereicht, in denen die Einwilligung erteilt

---

544 Vgl. Art. 2 lit. h DS-RL.

545 Vgl. § 4 Abs. 3 Satz 1 Nr. 1-3 BDSG.

546 So *Holznagel/Sonntag* in Roßnagel: Handbuch Datenschutzrecht, 2003, 4.8 Einwilligung des Betroffenen, Rn. 49.

wird, sodass es sich dabei um allgemeine Geschäftsbedingungen (AGB) handelt, die der AGB-rechtlichen Kontrolle nach den §§ 305 ff. BGB unterliegen.[547]

Dem Betroffenen müssen dabei unaufgefordert der konkrete Zweck der spezifischen Verarbeitung, Name und Anschrift des Verantwortlichen, eine geplante Übermittlung der Daten an Dritte, der Umfang der Speicherung, die Konsequenzen der Verweigerung der Einwilligung sowie alle sonstigen für die Beurteilung des Datenverarbeitungsvorgangs und seiner Konsequenzen erforderlichen Informationen mitgeteilt werden bzw. in den AGB enthalten sein.[548] Dabei muss jedoch das Hervorhebungsgebot des § 4a Abs. 1 Satz 4 BDSG beachtet werden.

Für den praktisch sehr relevanten Fall, dass ein Kraftfahrzeug nicht ausschließlich immer nur von ein und derselben Person gesteuert wird, hätte ein Fahrerwechsel auch für die verantwortliche Stelle im Hinblick auf die Erteilung einer wirksamen Einwilligung Auswirkungen. Wenn der Fahrer nicht mit dem Halter identisch ist, käme es in Betracht, dass die Hersteller den sein Kraftfahrzeug einem Dritten überlassenden Halter im Rahmen ihrer AGB dazu verpflichten, die Einwilligung des Dritten einzuholen.[549] Alternativ könnte dies jedoch auch auf technischer Ebene dahingehend gelöst werden, dass z.B. der Start des Kraftfahrzeuges nur möglich wäre, wenn zuvor die im Display erscheinende Einwilligungserklärung akzeptiert würde.

Auf europäischer Ebene enthält die Datenschutz-Grundverordnung auch bezüglich der Einwilligung Regelungen. Die Rechtmäßigkeit der Datenverwendung kann also auch hiernach durch Einwilligung des Betroffenen herbeigeführt werden, soweit dies den Anforderungen der Art. 6 Abs. 1 lit. a, Art. 7, 8 DS-GVO entspricht. Hinsichtlich der Einwilligung im Beschäftigungsverhältnis wird in Erwägungsgrund (43) DS-GVO festgestellt, dass eine Einwilligung nicht als Erlaubnistatbestand herangezogen werden kann, wenn zwischen der Position der betroffenen Person und des für die Verarbeitung Verantwortlichen ein klares Ungleichgewicht besteht. Der noch im Entwurf der Daten-

---

547 Denn obwohl es sich bei der Einwilligung nicht um eine „*Vertragsbedingung*“ handelt, die den Vertragsinhalt gestaltet, ist anerkannt, dass auch die Einwilligung unter § 305 Abs. 1 BGB zu subsumieren ist, soweit sie im Kontext einer vertraglichen Beziehung steht, vgl. *Tinnefeld/Buchner/Petri*: Einführung in das Datenschutzrecht, ^{5}2012, S. 348. Die Vorschrift des § 305 Abs. 1 Satz 1 BGB definiert Allgemeine Geschäftsbedingungen als alle für eine Vielzahl von Verträgen vorformulierten Vertragsbedingungen, die eine Vertragspartei (Verwender) der anderen Vertragspartei bei Abschluss eines Vertrags stellt.

548 Vgl. *Holznagel/Sonntag* in Roßnagel: Handbuch Datenschutzrecht, 2003, 4.8 Einwilligung des Betroffenen, Rn. 45.

549 Vgl. *Kinast/Kühnl*, NJW 2014, S. 3057–3061 (3059).

schutz-Grundverordnung vorgesehene pauschale Ausschluss von Einwilligungen im Beschäftigungsverhältnis[550] wurde zwischenzeitlich aufgegeben. Insoweit ergibt sich aus den Regelungen der Datenschutz-Grundverordnung nach Erlass keine ausdrückliche grundsätzliche Unbeachtlichkeit der Einwilligung des Arbeitnehmers im Rahmen des Beschäftigungsverhältnisses. Im Interesse der Betroffenen ist somit weiterhin die Erteilung einer Einwilligung auch im Beschäftigungsverhältnis möglich. Dies muss sich jedoch an den vorgenannten Aspekten orientieren und ist für jeden Einzelfall zu entscheiden.

2. Notwendigkeit der Einwilligung

Eine Einwilligung muss nicht eingeholt werden, wenn es sich bei den verwendeten Daten um anonymisierte Daten handelt.

Die Einwilligung sollte immer nur dann als Möglichkeit zur Legitimation einer Datenverwendung herangezogen und eingeholt werden, wenn feststeht, dass kein gesetzlicher Erlaubnistatbestand vorliegt, um letztlich der pauschalen Einwilligung in die Datenverwendung keinen Raum zu geben.[551]

Insbesondere im Zusammenhang mit Beschäftigungsverhältnissen sollte eine Einwilligung nur dann eingeholt werden, wenn tatsächlich kein anderer Erlaubnistatbestand greift. Es könnte ansonsten mit Einholung der Einwilligung der Eindruck erweckt werden, deren Verweigerung könne die Verarbeitung verhindern sowie die Freiwilligkeit der Einwilligung infrage stellen für den Fall, dass der Betroffene darauf hingewiesen wird, die Verarbeitung könne auch unter Anwendung einer Rechtsnorm erlaubt sein.[552]

---

550 Ein Ungleichgewicht sollte vor allem dann gegeben sein, wenn sich die betroffene Person in einem Abhängigkeitsverhältnis zu dem für die Verarbeitung Verantwortlichen befindet, zum Beispiel dann, wenn personenbezogene Daten von Arbeitnehmern durch den Arbeitgeber im Rahmen eines Beschäftigungsverhältnisses verarbeitet werden. In diesen Fällen sollte eine Einwilligung grundsätzlich unbeachtlich sein.

551 Vgl. *Taeger* in Taeger/Gabel: BDSG, [2]2013, § 4 BDSG, Rn. 48.

552 Vgl. *Weichert* in DKWW: Bundesdatenschutzgesetz, [4]2014, § 4, Rn. 4.

Nach Ansicht der Art. 29-Datenschutzgruppe soll dadurch eine Irreführung vermieden werden.[553]

Dieser Aspekt stellt in Bezug auf Beschäftigungsverhältnisse, im Rahmen derer vernetzte Fahrzeuge als Dienstfahrzeuge eingesetzt werden, eine große Herausforderung dar, wenn es darum geht, eine Datenverwendung daraus durch Einholung einer wirksamen Einwilligung zu rechtfertigen. An die Wirksamkeit einer solchen Einwilligung werden hohe Herausforderungen gestellt.

Es sollte in Bezug auf die Frage der Notwendigkeit einer Einwilligung immer auch im Blick behalten werden, dass diese als *„Schlüssel zu einem nahezu unbegrenzten, von allen ansonsten zu beachtenden gesetzlichen Schranken befreiten Zugang zu den von der verantwortlichen Stelle jeweils gewünschten Angaben“* führt.[554] Es besteht mithin die Gefahr, dass die Einwilligung hier nur noch als Instrument eingesetzt wird, um eine Datenverwendung so weit wie möglich zuzulassen.

3. Anforderungen an eine wirksame Einwilligung des Arbeitnehmers beim Einsatz vernetzter Kraftfahrzeuge

An dieser Stelle sind sodann die Anforderungen der vorgenannten allgemeinen Grundsätze auf die Erteilung einer wirksamen Einwilligung des Arbeitnehmers beim Einsatz vernetzter Fahrzeuge zu übertragen.

Vorangestellt sei, dass die Einwilligung als zentrales Rechtsinstrument grundsätzlich nicht auf mehrpolare Konstellationen zugeschnitten ist, wie sie insbesondere im Verhältnis des Arbeitgebers gegenüber dem Arbeitnehmer und zwischen Fahrern und Halter eines Kraftfahrzeugs vorliegen.[555]

---

553 *„Die Artikel 29-Datenschutzgruppe ist der Auffassung, dass es in den Fällen, in denen ein Arbeitgeber zwangsläufig aufgrund des Beschäftigungsverhältnisses personenbezogene Daten verarbeiten muss, irreführend ist, wenn er versucht, diese Verarbeitung auf die Einwilligung der betroffenen Person zu stützen. Die Einwilligung der betroffenen Person sollte nur in den Fällen in Anspruch genommen werden, in denen der Beschäftigte eine echte Wahl hat und seine Einwilligung zu einem späteren Zeitpunkt widerrufen kann, ohne dass ihm daraus Nachteile erwachsen“*, vgl. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_de.pdf.

554 Vgl. *Simitis* in Simitis: Bundesdatenschutzgesetz, [8]2014, § 4a, Rn. 4.

555 So *Schwartmann*, Sonderveröffentlichung zu RDV 3/2015, S. 3.

a) Kenntnis

Die Kenntnis des Arbeitnehmers vom Umgang mit seinen personenbezogenen Daten setzt voraus, dass dem Arbeitnehmer tatsächlich bewusst ist, dass Daten von ihm erhoben, verarbeitet und gespeichert werden, die einen Personenbezug aufweisen und durch die er identifiziert werden kann bzw. die auf ihn zurückzuführen sind. Insbesondere bei der Verwendung von Ortungstechnik in der Logistik- und Sicherheitsbranche ist dies nicht durchgängig der Fall.[556]

b) Freiwilligkeit

Die Problematik in diesem Bereich stellt sich jedoch vor allem hinsichtlich der Anforderungen an die Freiwilligkeit einer Einwilligung in die Datenverwendung seitens des Arbeitnehmers. Da das Arbeitsverhältnis für den Arbeitnehmer dessen Existenzgrundlage darstellt und er auf dieses angewiesen ist, steht er unter erheblichem Druck, eine Einwilligung zu erteilen, die er unabhängig vom Arbeitsverhältnis gar nicht erteilen würde.[557] Für ihn ist die Alternative, einen Arbeitsvertrag nicht abzuschließen, nicht verhandelbar. Er ist darauf angewiesen, dass er seinen Lebensunterhalt durch Aufnahme eines Arbeitsverhältnisses verdient und ist somit real nicht in der Position, die Einwilligung in die Datenverwendung zu verweigern. Denn für diesen Fall müsste er wohl damit rechnen, das Arbeitsverhältnis nicht eingehen zu können. Darin spiegelt sich der Konflikt wieder, der durch das im Arbeitsverhältnis bestehende Ungleichgewicht ausgelöst wird.

Diese beschriebene Asymmetrie im Arbeitsverhältnis zwischen Arbeitnehmer auf der einen und Arbeitgeber auf der anderen Seite wird auch durch die Rechtsprechung des Bundesverfassungsgerichts bestätigt. In einem Nichtannahmebeschluss hat das Bundesverfassungsgericht verdeutlicht, dass sich der *„einzelne Arbeitnehmer (...) beim Abschluss von Arbeitsverträgen typischerweise in einer Situation struktureller Unterlegenheit befindet“*.[558]

---

556 Vgl. https://www.datenschutzbeauftragter-info.de/ueberwachung-am-arbeitsplatz-gps-vs-datenschutz.

557 Vgl. *Büllesbach* in Roßnagel: Handbuch Datenschutzrecht, 2003, 6.1 Datenschutz in der betrieblichen Datenverarbeitung, Rn. 14.

558 So Bundesverfassungsgericht, Beschluss vom 23.11.2006, Aktenzeichen 1 BvR 1909/06, NJW 2007, S. 286-288.

Allerdings kann ohne Einzelfallprüfung nicht von einer generellen Einordnung der Einwilligung im Arbeitsverhältnis als unfreiwillig ausgegangen werden.

Zwar spricht wohl im Regelfall eine Vermutung dafür, dass eine seitens des Arbeitnehmers gegenüber dem Arbeitgeber erteilte Einwilligung in die Datenverwendung unfreiwillig ist.[559] Dies kann jedoch im Wege einer Einzelfallprüfung durch das Vorliegen besonderer Umstände widerlegt werden. Dies ist beispielsweise dann möglich, wenn die Einwilligung dem Arbeitnehmer objektiv überwiegend deutliche Vorteile verschafft.[560] Die Beweislast dafür, dass die getroffene Regelung erforderlich ist und der Abschluss des Arbeitsvertrages ausdrücklich nicht die Erteilung einer Einwilligung voraussetzt, weil seitens des Arbeitgebers sanktionsfreie Wahlmöglichkeiten geboten werden, trägt jedoch der Arbeitgeber.[561] Zudem soll der Betroffene nach dem Verständnis des Bundesdatenschutzgesetzes generell in der Lage sein, eine eigenverantwortliche Entscheidung über die Verwendung seiner personenbezogenen Daten zu treffen und dadurch sein Recht auf informationelle Selbstbestimmung auszuüben.[562] Auch dieser Aspekt ist mit einer grundsätzlichen Unmöglichkeit der Erteilung einer Einwilligung im Arbeitsverhältnis nicht zu vereinbaren.

Insgesamt ist darauf zu achten, dass die notwendige Transparenz hergestellt wird. Es wird oftmals von Seiten des Arbeitgebers nicht umfänglich aufgeklärt. Erschwerend kommt im vorliegenden Kontext dazu, dass auch im Hinblick auf die komplexe Technologie vernetzter Fahrzeuge auch von Seiten des Arbeitgebers meist nicht die Voraussetzungen vorliegen, um die nötige Transparenz herzustellen. Sofern auch dem Arbeitgeber nicht bekannt ist, welche Daten aus dem vernetzten Fahrzeug verwendet werden, ist es ihm insoweit unmöglich, hierüber ausreichend aufzuklären.

Insgesamt muss also im Einzelfall gefragt werden, ob die Willensbildung des Betroffenen bezüglich der Einwilligung in die Datenverwendung tatsächlich freiwillig erfolgt oder durch zu befürchtende berufliche Nachteile eingeschränkt oder beeinflusst wird. Sobald dies in unangemessener Weise passiert, kann im Rahmen des Arbeitsverhältnisses nicht mehr von einer freien Entscheidung des Betroffenen ausgegangen werden. Dies hat zur Folge, dass eine unter solchen Voraussetzungen erteilte Einwilligung als unwirksam einzustufen ist. Die Datenverwendung ist in diesem Fall unzulässig. Denn

559 So *Däubler* in DKWW: Bundesdatenschutzgesetz, [4]2014, § 4a, Rn. 23.
560 Vgl. *Hilbrans* in DHSW: Arbeitsrecht, [3]2013, § 4a BDSG; Rn. 3.
561 So *Wedde*, DuD 2004, S. 169-174 (172).
562 So *Riesenhuber*, RdA 2011, S. 257-265 (261).

ein Rückgriff auf gesetzliche Erlaubnistatbestände ist wie vorgenannt für den Fall, dass eine erteilte Einwilligung sich als unwirksam erweist, ausgeschlossen.

Aber selbst bei formal wirksamer erteilter Einwilligung sind inhaltliche Schranken zu beachten. So dürfen auch mit Einwilligung des betroffenen Arbeitnehmers keine Persönlichkeitsprofile erstellt werden, die auf Details seines Arbeitsverhaltens und seiner Kommunikation mit Arbeitskollegen und Vorgesetzten schließen lassen.[563]

c) Gültigkeitsdauer

Eine generelle Frage stellt sich in diesem Zusammenhang auch im Hinblick auf die Gültigkeitsdauer einer einmal erteilten Einwilligung. Unabhängig davon, dass eine Einwilligung grundsätzlich unbefristet gelten soll[564], kommt es bei dieser Frage vorwiegend auf die Ausgestaltung des konkreten Einzelfalls an.

Im Arbeitsverhältnis werden über den gesamten Zeitraum der Beschäftigung personenbezogene Daten verwendet. Meist werden auch schon vor Beginn der Beschäftigung Daten erhoben, die die Einstellung der Person betreffen. Soweit die Verwendung der personenbezogenen Daten dem Bestand und der Verwaltung des Beschäftigungsverhältnisses dienen, könnte hier angenommen werden, eine einmal erteilte Einwilligung gelte bis zur Beendigung des Beschäftigungsverhältnisses. Je nach Ausgestaltung des Einzelfalls wurde bereits höchstrichterlich geurteilt, dass eine auf einer Einwilligung des Arbeitnehmers beruhende Befugnis des Arbeitgebers nicht automatisch mit der Beendigung des Arbeitsverhältnisses erlischt.[565]

Dies könnte sich jedoch in den Fällen anders darstellen, in denen Daten erhoben und verwendet werden, die darauf angelegt sind, nur für einen bestimmten Zweck zur Verfügung zu stehen. Eine darauf gerichtete Einwilligung kann insoweit gerade nicht unbegrenzt bzw. für die gesamte Dauer des Beschäftigungsverhältnisses Geltung beanspruchen.

---

563 So *Däubler*: Gläserne Belegschaften?, ^{6}2015, Rn. 120.

564 So *Plath* in Plath: BDSG, 2013, § 4a, Rn. 21.

565 Mit Urteil vom 19.02.2015, Aktenzeichen 8 AZR 1011/13, AuR 2015, S. 158 entschied das Bundesarbeitsgericht, dass für den Widerruf einer Einwilligung nach Beendigung des Arbeitsverhältnisses ein plausibler Grund vorliegen müsse, soweit es um die Einwilligung zur Verwendung eines Films zu Werbezwecken gehe, der auf der Unternehmerwebsite abrufbar gewesen sei. Die nach § 22 KUG erforderliche Einwilligung sei erteilt worden und habe keine Begrenzung der Veröffentlichung auf die Dauer des Arbeitsverhältnisses enthalten. Auch ein plausibler Grund für den Widerruf sei nicht vorgetragen worden.

Insbesondere im Hinblick auf vernetzte Fahrzeuge im Flottenbereich muss Berücksichtigung finden, dass sich die Technik und somit auch die Möglichkeiten der Datengewinnung rasant weiterentwickeln. Es würde den Schutz des Arbeitnehmers einengen, wenn eine Einwilligung zur Verwendung der Daten aus seinem Fahrzeug – einmal erteilt – zeitlich uneingeschränkt für die Zukunft gelten könnte. Es ist damit zu rechnen, dass in den kommenden Jahren immer mehr technische Möglichkeiten bereitgestellt werden, um z.B. Persönlichkeitsprofile zu generieren und dies insoweit zum *„gläsernen Arbeitnehmer“* führen könnte. Diese Aspekte sprechen hier jedoch gerade dagegen, dem Arbeitgeber die Möglichkeit zu eröffnen, einmal eine Einwilligung einzuholen und von dieser ohne Anpassung an geänderte Umstände für die gesamte Dauer des Beschäftigungsverhältnisses Gebrauch zu machen. Die Einwilligung müsste hier in wiederkehrenden Zeitabschnitten erneuert werden.

Dazu könnte man sich orientieren an der Rechtsprechung, die allgemein zur Gültigkeitsdauer einer erteilten Einwilligung existiert. Diese betrifft vorwiegend Fälle, in denen es um die Einwilligung zur Datenverwendung für E-Mail-Newsletter geht. Das Landgericht München entschied mit Urteil vom 08.04.2010[566], dass eine erteilte Einwilligung nach anderthalb Jahren ihre Aktualität verloren habe und deshalb nicht mehr als Rechtfertigung für die werbliche Nutzung der E-Mail-Adresse des Betroffenen herangezogen werden könne. Zuzustimmen ist ebenfalls einer Entscheidung des Landgerichts Berlin[567], wonach eine nicht genutzte Einwilligungserklärung nach spätestens zwei Jahren ihre Wirksamkeit verliere und es nach Ablauf dieses Zeitraumes und der Nichtnutzung der Erklärung einer neuen Einwilligungserklärung bedürfe.

Insgesamt ist im vorliegenden Zusammenhang also tatsächlich die erteilte Einwilligung in bestimmten Zeitabständen zu aktualisieren. Zu empfehlen ist hier insbesondere im Hinblick auf den schnellen technischen Fortschritt ein Zeitraum von anderthalb Jahren.

---

566 Landgericht München, Urteil vom 08.04.2010, Aktenzeichen 17 HK O 138/10, CR 2011, S. 830; das Urteil betrifft eine wettbewerbsrechtliche Angelegenheit und die Frage, ob in der Versendung des Newsletters eine unzumutbare Belästigung im Sinne des § 7 UWG zu sehen ist. Der Grundgedanke, dass eine einmal erteilte Einwilligung nicht zeitlich unbegrenzt genutzt werden darf, ist jedoch hierher zu übertragen.

567 Landgericht Berlin, Beschluss vom 02.07.2004, Aktenzeichen 15 O 653/03, NJW-RR 2004, S. 1631-1633.

d) Möglichkeit des Rückgriffs auf gesetzliche Erlaubnistatbestände

In Frage steht auch, ob im Falle einer erteilten Einwilligung noch ein Rückgriff auf die gesetzlichen Erlaubnistatbestände möglich sein soll.

Hierzu könnte man die Auffassung vertreten, ein Rückgriff auf die gesetzlichen Erlaubnistatbestände sei auch dann noch möglich, wenn eine erteilte Einwilligung aus verschiedenen Gründen wegfällt. So hat das Oberlandesgericht Frankfurt am Main entschieden[568], dass selbst im Falle einer unwirksamen Einwilligung die Datenverwendung im Streitfall nach den gesetzlichen Erlaubnistatbeständen gerechtfertigt sein kann.

Eine solche Bevorteilung der verantwortlichen Stelle kann insbesondere im Rahmen von Beschäftigungsverhältnissen nicht akzeptiert werden. Denn in Anlehnung an die Stellungnahme der Artikel 29-Datenschutzgruppe[569] muss in solchen Fällen eine Irreführung des Arbeitnehmers unbedingt vermieden werden. Diese würde sich unter Anwendung der durch die Rechtsprechung des Oberlandesgerichts Frankfurt am Main aufgestellten Grundsätze gerade einstellen. Denn der Arbeitnehmer hat hier nur scheinbar eine Wahl, seine Einwilligung zu erteilen. Er geht davon aus, dass er durch die Entscheidung über die Erteilung einer Einwilligung tatsächlich frei entscheiden kann, ob es zu einer Datenverwendung kommt. Wenn jedoch im Falle eines Widerrufs der Einwilligung ohne weiteres auf die gesetzlichen Erlaubnistatbestände zurückgegriffen werden dürfte, spielte im Ergebnis die Einwilligung des Betroffenen keine Rolle mehr. Dann läge es gerade nicht allein in seiner Entscheidungsgewalt, ob es zu einer Datenverwendung kommt. Dem Betroffenen wird allerdings durch das Einholen einer Einwilligung suggeriert, er könne aufgrund seines ihm zustehenden Rechts auf informationelle Selbstbestimmung eigenständig über die Datenverwendung entscheiden. Insoweit kann auch von einer Täuschung des Betroffenen gesprochen werden, wenn die Daten trotz Widerrufs der Einwilligung weiterhin verwendet werden.[570] Auch der auf dem Grund-

---

568 Oberlandesgericht Frankfurt am Main, Beschluss vom 13.07.2010, Aktenzeichen 19 W 33/10, MMR 2010, S. 792-793; in der Sache war zu beurteilen, ob die Übermittlung von Daten zu einer rechtskräftig titulierten Forderung an die SCHUFA regelmäßig nach § 28 Abs. 1 Nr. 2 BDSG (a.F.) zulässig ist. Durch die BDSG-Novelle II 2009 wurde der neue § 28a BDSG in das Bundesdatenschutzgesetz eingefügt, der die Übermittlung personenbezogener Daten über eine Forderung an Auskunfteien unter den dort genannten Voraussetzungen zulässt.

569 Vgl. *Stellungnahme 8/2001 der Artikel 29-Datenschutzgruppe zur Verarbeitung personenbezogener Daten von Beschäftigten vom 13.09.2001*, 5062/01/DE/endg. WP 48, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_de.pdf; vgl. insoweit auch unter *Kapitel 3, Teil 3, II.2.*.

570 Vgl. *Scholz/Sokol* in Simitis: Bundesdatenschutzgesetz, [8]2014, § 4, Rn. 6.

satz von Treu und Glauben beruhende Einwand des Rechtsmissbrauchs steht einer solchen Vorgehensweise entgegen, wenn die Einwilligung unter Ausnutzung einer wirtschaftlichen Machtposition *„abgepresst“* oder durch arglistige Täuschung erschlichen wurde.[571] Der Arbeitgeber als verantwortliche Stelle hat hier Rücksicht zu nehmen auf die Interessen des Arbeitnehmers. Gerade das Beschäftigungsverhältnis ist geprägt von einer Vertrauensbasis. Dem steht es jedoch entgegen, wenn die verantwortliche Stelle nur rein vorsorglich eine Einwilligung einholt und den Arbeitnehmer in dem Glauben lässt, er könne selbst entscheiden, ob es zu einer Datenverwendung kommt, um nach einem etwaigen Widerruf oder der Kenntnis von der Unwirksamkeit der Einwilligung auf die gesetzlichen Erlaubnistatbestände zurückzugreifen.

Der Problematik kann im Ergebnis jedoch nur so begegnet werden, dass bei einer einmal erteilten Einwilligung ein Rückgriff auf die gesetzlichen Erlaubnistatbestände für den Fall des Widerrufs oder der Unwirksamkeit der Einwilligung ausgeschlossen sein soll. Wenn eine Einwilligung also einmal erteilt wurde, ist die verantwortliche Stelle auf deren Wirksamkeit komplett angewiesen. Nur so kann das bestehende klare Ungleichgewicht im Rahmen des Beschäftigungsverhältnisses berücksichtigt werden.

III. Spezialgesetzliche Erlaubnistatbestände

Im Rahmen des Beschäftigtendatenschutzes und auch im Hinblick auf die sich rasant weiterentwickelnde Technik insbesondere im Bereich der Telekommunikation in Verbindung mit der Vernetzung derselben mit dem Kraftfahrzeug sowie mit anderen intelligenten Verkehrssystemen müssen etwaige vorrangige spezialgesetzliche Vorschriften im Sinne des § 1 Abs. 3 BDSG beachtet werden. Die Vorschriften des Bundesdatenschutzgesetzes sind insoweit subsidiär, als speziellere Erlaubnistatbestände vorhanden sind. Auch hieraus können sich Erlaubnistatbestände neben den gesetzlich geregelten des Bundesdatenschutzgesetzes sowie neben der Einwilligung ergeben. Diese finden sich für den Datenschutz bei Telekommunikation- und Internetnutzung im Rahmen des Beschäftigungsverhältnisses in den bereichsspezifischen Vorschriften des Telekommunikationsgesetzes (TKG) und des Telemediengesetzes (TMG)[572].

---

571 So *Gola*, RDV 2002, S. 109–116 (110).

572 Das Telemediengesetz ersetzt seit dem Jahr 2007 das Teledienstegesetz (TDG) und das Teledienstedatenschutzgesetz (TDDSG) und wurde als Art. 1 des Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz (ElGVG) eingeführt; vgl. dazu BGBl. I 2007, Nr. 6 vom 28.02.2007, S. 179 sowie *Roßnagel* in Roßnagel: Beck'scher Kommentar zum Recht der Telemediendienste, 2013, Einf, Rn. 25.

Aus technischer Sicht betrifft diese Thematik die Integration des Mobiltelefons oder sonstiger technischer Geräte in das Kraftfahrzeug, was unter den Begriff des sog. *„Mobile Computing“* zu fassen ist. Darunter versteht man den Zugriff mit einem mobilen Kommunikationsgerät auf ein zentrales Informationsgerät, bei dem alle Tätigkeiten ausgeführt werden können, ohne von einem festen Standort abhängig zu sein.[573] Dies ermöglicht insbesondere die Integration von Infotainment-Angeboten und Apps im Kraftfahrzeug. Dem Fahrer können dadurch individuell auf ihn abgestimmte Programme zur Verfügung gestellt werden, die er dann sowohl im Kraftfahrzeug aber auch unabhängig davon beispielsweise auf seinem Mobiltelefon nutzen kann. Durch diese Integration ist es technisch mittlerweile auch möglich, dem Fahrer in Form sog. *„Local Based Services“* (LBS)[574] im Zusammenhang mit der Nutzung des Mobilfunkgeräts und des Navigationsgeräts und den daraus generierten Daten individuelle Angebote zu präsentieren und ihm sog. POI aufzuzeigen, auf die er sodann zugreifen und die für ihn günstigen Angebote wahrnehmen kann.[575] Er kann selbst bestimmen, welche ihm angebotenen Unterhaltungs- und Serviceangebote für ihn von Relevanz sind.

Auch im Bereich des Beschäftigtenverhältnisses kann dies eine Rolle spielen. Oftmals wird dem Beschäftigten ein Dienstfahrzeug zur Verfügung gestellt, welches im Eigentum der verantwortlichen Stelle steht. Wird in diesen Fällen während der Fahrt auf intelligente Verkehrssysteme zurückgegriffen, stellt sich die Frage, ob dies die Anwendbarkeit des Telekommunikationsgesetzes oder des Telemediengesetzes auszulösen vermag und dadurch die Subsidiarität der Vorschriften des Bundesdatenschutzgesetzes greifen könnte.

1. Telekommunikationsgesetz

Im Bereich der Telekommunikation stellt § 91 Abs. 1 Satz 1 TKG die zentrale Vorschrift dar. Danach werden personenbezogene Daten von Teilnehmern und Nutzern[576] von Telekommunikation bei der Datenverwendung durch die verantwortliche Stelle

---

573 Vgl. *Roberts*: Gabler-Wirtschafts-Lexikon, Band L-O, [17]2010, Stichwort *"Mobile Computing"*, S. 2105.

574 Diese standortbezogenen Dienste stellen als mobile Dienste unter Zuhilfenahme positionsabhängiger Daten von Endnutzern selektive Informationen bereit, vgl. https://de.wikipedia.org/wiki/Standortbezogene_Dienste.

575 Vgl. zu diesem Komplex unter *Kapitel 2, Teil 4*.

576 Als Nutzer ist derjenige zu qualifizieren, welcher einen Dienst rein faktisch in Anspruch nimmt, vgl. *Moos* in Taeger/Gabel: Kommentar zum BDSG, [2]2013, § 11 TMG, Rn. 25.

geschützt, die geschäftsmäßig Telekommunikationsdienste erbringen oder an deren Erbringung mitwirken.[577]

Auch telekommunikationsgestützte Dienste nach § 3 Abs. 25 TKG, die keinen räumlich oder zeitlich trennbaren Leistungsfluss auslösen, sondern bei denen die Inhaltsleistung noch während der Telekommunikationsverbindung erfüllt wird, sind im Umkehrschluss aus § 1 Abs. 1 Satz 1 TMG vom Anwendungsbereich des Telekommunikationsgesetzes umfasst.[578]

Da nach dem Stand der Technik heutzutage eine Verschmelzung einzelner Infrastrukturen, wie z.B. des Mobiltelefons und des Internets bereits vorliegt und scheinbar unaufhaltsam weiterschreitet, muss anhand einer wertenden Gesamtbetrachtung der maßgebliche Schwerpunkt eines bestimmten Dienstes bestimmt werden.[579] Telekommunikationsdienste nach § 3 Abs. 24 TKG umfassen somit nur die technische Seite der Übertragung.[580] Gemeint ist damit der reine Transport der Daten, ohne dass eine inhaltliche Überprüfung stattfindet.

Im Rahmen intelligenter Verkehrssysteme werden einige Daten über das Mobilfunknetz zur Verfügung gestellt. Darin ist eine Übertragung von Signalen über Telekommunikationsnetze zu sehen, die sodann den Vorschriften des Telekommunikationsgesetzes, dort den §§ 91 ff. TKG unterliegt.

Sofern der Anwendungsbereich der §§ 91 ff. TKG eröffnet ist, ergeben sich daraus für die Verwendung von Daten aus Signalübertragungen im Rahmen intelligenter Verkehrssysteme entscheidende Einschränkungen. Eine Datenverwendung ist für bestimmte Daten dann nur noch bei Vorliegen einer Einwilligung möglich.

---

577 Telekommunikationsdienste sind gemäß § 3 Abs. 24 TKG legaldefiniert als in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen. Ein geschäftsmäßiges Erbringen von Telekommunikationsdiensten liegt nach der Definition des § 3 Abs. 10 TKG vor bei einem nachhaltigen Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht.

578 Denn aus § 1 Abs. 1 Satz 1 TMG ergibt sich, dass die Vorschriften des Telemediengesetzes nur gelten, soweit es sich nicht um Telekommunikationsdienste nach § 3 Abs. 24 TKG oder um telekommunikationsgestützte Dienste im Sinne des § 3 Abs. 25 TKG handelt. Es erfolgt mithin eine Negativabgrenzung nach § 1 Abs. 1 Satz 1 TMG.

579 Eine andere Möglichkeit besteht darin, jedes abgrenzbare Teilangebot separat zu betrachten und einzuordnen; vgl. *Tinnefeld/Buchner/Petri*: Einführung in das Datenschutzrecht, [5]2012, S. 213.

580 Vgl. *Ricke* in Spindler/Schuster: Recht der elektronischen Medien, [3]2015, § 3 TKG, Rn. 43.

Auf europäischer Ebene gilt für diese Daten die sog. *„E-Privacy-Richtlinie“*[581]. Die Datenschutz-Grundverordnung gibt hierzu bislang keine Regelungen vor. Es sollte somit auch für den Datenschutz im Telekommunikationsbereich eine vereinheitlichende Verordnung nach dem Beispiel der Datenschutz-Grundverordnung in die Wege geleitet werden.

Im Zusammenhang mit vernetzten Fahrzeugen hat sich der Automobilhersteller BMW bereits gemäß § 6 TKG als Telekommunikationsdiensteanbieter bei der Bundesnetzagentur registrieren lassen.[582]

2. Telemediengesetz

Sollte hingegen die Anwendbarkeit des Telemediengesetzes eröffnet sein[583], ergeben sich ebenfalls erhebliche Einschränkungen für die verantwortliche Stelle. Das Telemediengesetz gilt für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste oder Rundfunk sind. Unter anderem sollen Funktionalitäten, wie z.B. Datendienste (Verkehr, Wetter, Umwelt, Börse), Empfehlungs- und Ratgeberdienste, Bestellungs-, Buchungs- und Maklerdienste, einschließlich Shops und Handelsplattformen, Presse und Nachrichtendienste sowie On-Demand- und Streaming-Dienste gerade als Telemediendienste eingestuft und in diesen Fällen der Anwendungsbereich des Telemediengesetzes eröffnet werden.[584] Auch die bereits erwähnten Local Based Services lassen sich als klassische elektronische Informationsdienste als Dienste im Sinne des Telemediengesetz einordnen.[585]

Dies hat zur Folge, dass insoweit die §§ 11 ff. TMG anzuwenden sind. Nach § 13 TMG treffen den Diensteanbieter vielfältige Unterrichtungspflichten, denen er durch Überlas-

---

581 *Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)*, ABl. Nr. L 201 vom 31.07.2002, S. 37-47.

582 Vgl. http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/Meldepflicht/TKDiensteanbieterPDF.pdf?__blob=publicationFile&v=28.

583 Dies gilt insbesondere im Hinblick auf intelligente Verkehrssysteme, die man aufgrund der Überschneidung im Wortlaut des § 2 Nr. 1 IVSG einerseits und des § 1 Abs. 1 Satz 1 TMG andererseits vereinfacht als Telemedien im Fahrzeug einstufen kann, vgl. dazu *Schwartmann*, Sonderveröffentlichung zu RDV 3/2015, S. 6.

584 Nicht abschließende Aufzählung nach *Kremer*, RDV 2014, S. 240–252 (247).

585 Vgl. *Tinnefeld/Buchner/Petri*: Einführung in das Datenschutzrecht, ^{5}2012, S. 214.

sung einer Datenschutzerklärung Rechnung tragen muss, in welche der Nutzer einwilligen muss.

Aufgrund der bereits aufgezeigten Verschmelzung von Infrastrukturen wird es fortlaufend schwieriger werden, eine genaue Einordnung zu treffen, ob es sich bei dem betreffenden Dienst um einen Telemediendienst oder aber um Telekommunikation handelt. Diese Entwicklung ist auch im Bereich intelligenter Verkehrssysteme zu beobachten, sodass diese je nach ihrer Art sowohl als Telemediendienst als auch als Telekommunikation eingeordnet werden können. Eine Subsumtion ist somit unter das Telemediengesetz ebenso denkbar wie unter das Telekommunikationsgesetz. Für eine genaue Einordnung müssten die einzelnen Dienste separat überprüft werden. An dieser Stelle ist allerdings aufgrund des begrenzten Umfangs der Untersuchung festzuhalten, dass intelligente Verkehrssysteme ihrer Natur nach in den Anwendungsbereich beider Spezialgesetze fallen können.

a) Art der Nutzung des Dienstfahrzeugs

Es ist sodann zu differenzieren zwischen rein betrieblicher, privater und auch-privater Nutzung des Dienstfahrzeugs. Dies orientiert sich maßgeblich an der Vorschrift des § 11 TMG.[586] Bei ausschließlich betrieblicher bzw. dienstlicher Nutzung des Telemediendienstes in Gestalt des Dienstfahrzeugs ist somit ein Rückgriff auf die Erlaubnistatbestände des Bundesdatenschutzgesetzes vorzunehmen. Die Vorschriften der § 12 bis 15a TMG finden keine Anwendung.

b) Private und dienstliche Nutzung

Etwas anderes gilt jedoch für den Fall, dass dem Nutzer auch die private Nutzung des Dienstes seitens des Arbeitgebers als Diensteanbieter gestattet ist. Dann richtet sich die Zulässigkeit gerade nach den spezialgesetzlichen Regelungen und Erlaubnistatbeständen des Telemediengesetzes. Zurückzuführen ist dies auf das in § 11 TMG geregelte Anbieter-Nutzer-Verhältnis. Dies setzt voraus, dass der Arbeitnehmer Nutzer des Dienstes und der Arbeitgeber als Diensteanbieter einzustufen ist.

Daran fehlt es allerdings gerade für die Fälle, in denen eine rein betriebliche Nutzung des Dienstes vorliegt. Denn dann ist davon auszugehen, dass es sich bei dem Arbeitge-

---

586 Danach kommen die Vorschriften des 4. Abschnitts des Telemediengesetzes den Datenschutz betreffend gerade nicht zur Anwendung, soweit die Bereitstellung von Telemediendiensten im Dienst und Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken erfolgt, vgl. § 11 Abs. 1 Nr. 1 TMG.

ber um den Nutzer handelt, dem der Dienst zugutekommt und eben gerade nicht der Arbeitnehmer Nutzer sein soll.[587] Dem Arbeitnehmer steht der Dienst lediglich im Rahmen seiner beruflichen Tätigkeit und nur zur Erfüllung seiner Pflichten aus dem Arbeitsverhältnis zur Verfügung. Eine private Nutzung ist in solchen Fällen ausgeschlossen. Die Daten aus solchen Diensten stehen allein dem Arbeitgeber zur Verfügung. Er macht sich diese zu Nutze, sodass er selbst als Nutzer einzustufen ist. Da der Arbeitnehmer die Daten nicht zu privaten Zwecken nutzen darf, bietet der Arbeitgeber ihm diese auch nicht im Sinne des § 11 TMG an.

Sobald die Nutzung dagegen nicht nur rein betrieblich, sondern gerade auch zu privaten Zwecken erfolgen darf, finden im Umkehrschluss die einschränkenden Vorschriften der §§ 12 ff. TMG Anwendung. Dies führt auf Seiten des Arbeitgebers zu einem weitgehenden Kontrollverbot und dazu, dass er anfallende Daten lediglich für technische Betriebszwecke sowie zur Gewährleistung der Datensicherheit oder zu Abrechnungszwecken vorübergehend speichern darf.[588] Für den Fall, dass dem Arbeitnehmer auch die private Nutzung gestattet wird, sollte dies technisch so gestaltet werden, dass private und betriebliche Nutzung eindeutig zu differenzieren sind und somit eine Abrechnung der privaten Nutzung für den Arbeitgeber als Diensteanbieter möglich bleibt.[589]

Zuletzt ist zu beachten, dass für die Betroffenen hier auch die nötige Transparenz hergestellt werden muss. Nach § 13 TMG hat er den Nutzer zu Beginn des Nutzungsvorganges über Art, Umfang und Zweck der Datenverwendung und über eine Verarbeitung außerhalb Europas in allgemein verständlicher Form zu unterrichten. Den Diensteanbieter treffen hier vielfältige Transparenzpflichten.[590] Die Masse an Informationen müssen dem Verbraucher verständlich erteilt werden. Dass die derzeitige Praxis, alle erforderlichen Informationen in AGB zusammenzufassen, optimiert werden muss, wurde bereits

---

587 Vgl. *Spindler/Nink* in Spindler/Schuster: Recht der elektronischen Medien, [3]2015, § 11 TMG, Rn. 25.

588 Vgl. *Zilkens*, DuD 2005, S. 253–261 (254).

589 Beim Mobiltelefon kann dies darüber gelöst werden, dass ein Mobiltelefon zur Verfügung gestellt wird, welches die Möglichkeit bietet, zwei SIM-Karten einzulegen, um dadurch private und dienstliche Nutzung unterscheiden zu können. Hinsichtlich der betrieblichen Nutzung eines Kraftfahrzeugs kann dem Arbeitgeber aufgegeben werden, privat zurückgelegte Strecken zu dokumentieren. In beiden Fällen ist jedoch ein Missbrauch seitens des Arbeitnehmers nicht auszuschließen. Eine Missbrauchskontrolle kann jedoch unter Umständen als Zweckbestimmung der Datenverwendung im Arbeitsverhältnis gerechtfertigt sein. Zudem unterliegt die Missbrauchskontrolle den Voraussetzungen des § 100 Abs. 3 TKG, wonach eine Kontrolle bei Vorliegen tatsächlicher und dokumentierter Anhaltspunkte für eine rechtswidrige Inanspruchnahme von Telekommunikationsdienstleistungen erforderlich erscheint.

590 Weitere Regelungen finden sich in den §§ 5, 6, 13 Abs. 3, Abs. 5, 15 Abs. 3 TMG.

festgestellt. Der Verbraucher muss sensibel dafür gemacht werden, was mit seinen Daten passiert. Seitenlange AGB werden im Zweifel vom Verbraucher weder gelesen noch in Gänze verstanden. Ein Lösungsansatz könnte jedoch darin zu sehen sein, dass die Informationen nur noch situationsbezogen und nur dann erteilt werden, wenn sie erforderlich sind und gerade nicht vorab pauschal.[591]

Teil 4: *Wem „gehören" die Daten?*

I. Problemaufriss

Nachdem nunmehr die technischen und rechtlichen Grundlagen aufgezeigt wurden, soll der Blick auf die zentrale Frage gerichtet werden, die im Zusammenhang mit der Verwendung von Daten aus vernetzten Fahrzeugen im Rahmen sämtlicher Diskussionen derzeit aufgeworfen wird:

„Wem gehören die Daten?"[592]

„Gehören" meint nach dem allgemeinen Sprachgebrauch *„besitzen, innehaben, verfügen über oder sein Eigen nennen"*.[593] Aus rechtlicher Sicht muss danach eine Einordnung unter die Vorschriften der Eigentums- und Besitzschutzrechte erfolgen. Es ist zu fragen, wer berechtigt ist, über die Daten zu verfügen und andere von einer Nutzung auszuschließen.

Nachdem bereits geklärt werden konnte, welche Daten im vernetzten Fahrzeug überhaupt anfallen und insbesondere durch die Anwendung von Big Data generiert werden, stellt sich die Frage, wer eine Zugriffsbefugnis auf die anfallenden Daten hat. Dazu ist es jedoch erforderlich, den Blick nicht nur auf das Datenschutzrecht zu richten, das insoweit nur Zugriffs- und Verwendungsbefugnisse regelt, sondern vielmehr darüber hinaus nach einer Eigentumsposition für Daten zu suchen.

---

591 So *Weichert*, vgl. https://www.datenschutzzentrum.de/vortraege/20131112-weichert-schutzregelungen-tkg-bdsg.html.

592 Vgl. dazu beispielsweise nur http://www.verkehrswachtstiftung.de/news/wem-gehoeren-die-fahrzeugdaten.html; http://www.versicherungsbote.de/id/4813081/Telematik-Tarif-Kfz-Versicherung-ADAC-Kfz-Telematik/; http://www.car-it.com/rechtsfreier-raum-wem-gehoeren-die-daten-aus-dem-auto/id-0039081; http://www.morgenweb.de/nachrichten/vermischtes/wem-gehoren-fahrzeugdaten-1.1381526; vgl. auch *Bönninger*, zfs 2014 S. 184–189.

593 Vgl. http://www.duden.de/rechtschreibung/gehoeren.

Allerdings scheint die Frage, wem die Daten *„gehören“*, nicht richtiger Anknüpfungspunkt für eine Untersuchung zu sein. Es müsste insoweit bereits vorher angesetzt und untersucht werden, ob die Daten überhaupt rechtlich geschützt sind, dass sie überhaupt jemandem *„gehören“* können. Denn bislang existiert keine gesetzliche Regelung dazu, wem Daten gehören.

Um hier jedoch eine Einordnung vornehmen zu können, erscheint es sinnvoll zu differenzieren. Die Frage, ob Daten rechtlich geschützt sind und jemandem *„gehören“* können, betrifft den Schutz „*von“* Daten. Im Gegensatz dazu steht der Schutz „*vor“* Daten, der den Kern des Datenschutzrechtsrechts bildet und die Frage stellt, ob jemandem Zugriffsbefugnisse auf Daten zustehen und wie ein Betroffener vor zu vielen Daten geschützt werden kann.

II. Schutz von Daten

Zunächst soll jedoch die in der öffentlichen Diskussion im Mittelpunkt stehende Frage gestellt werden, ob die Daten aus dem vernetzten Fahrzeug überhaupt jemandem *„gehören“* können und ob diese Daten aus rechtlicher Sicht geschützte Rechtspositionen darstellen. *„Gehören“* meint hier eine Zuordnung der Daten als Eigentum oder eigentumsähnliche Position. Die Relevanz dieser Frage erklärt sich vor allem mit der Vielzahl an Interessengruppen, die bestimmte Daten für sich sozusagen exklusiv nutzen wollen. Ansprüche an Daten werden insbesondere von Autobanken, Versicherungen und Anbietern von Internetdiensten angemeldet.[594]

Festzustellen ist zunächst, dass es in einer Diskussion, wem Daten *„gehören“*, nur um solche Daten gehen kann, die tatsächlich Personenbezug aufweisen. Nicht personenbezogene Daten können bereits ihrer Art nach keiner Person zugeordnet werden und aufgrund dessen in der Folge auch keine eigentumsrechtliche oder eigentumsähnliche Position rechtfertigen.

1. Eigentum an Daten

Um jedoch andere von jeder Einwirkung auf die Daten ausschließen zu können und nur exklusiv das Recht ausüben zu können, mit den Daten nach Belieben zu verfahren, müsste eine zumindest eigentumsähnliche Position an Daten bestehen können. Diese

[594] Vgl. http://www.car-it.com/heikle-datenstroeme-wem-gehoeren-die-daten-aus-dem-fahrzeug/id-0038906.

könnte sich aus den Vorschriften des Bürgerlichen Gesetzbuches, des Bundesdatenschutzgesetzes sowie den Vorschriften des Urheberrechts ableiten lassen. Anhand dieser Vorschriften kann sodann untersucht werden, ob Daten im Allgemeinen und Daten aus vernetzten Fahrzeugen im Besonderen überhaupt eigentumsfähig sind.

Dazu muss jedoch zunächst geklärt werden, ob es sich bei Daten überhaupt um Sachen im rechtlichen Sinne handelt. Dies wird überwiegend abgelehnt mit der Begründung, Daten seien ebenso wie Computerprogramme das Ergebnis einer geistigen Schöpfung des Urhebers und deshalb als Immaterialgut einzustufen.[595] Lediglich bei Verkörperung in einem Datenträger soll nach der Rechtsprechung des Bundesgerichtshofs[596] die Sacheigenschaft bejaht werden. Daran schließt sich auch die von *Boehm*[597] vorgenommene Differenzierung nach Art der Daten an. Während danach einerseits sog. strukturelle Daten existierten, die auf einem Speichermedium, wie z.B. einer Festplatte oder einer CD zu finden seien, seien andererseits die sog. syntaktischen Daten wie Codes und technische Datensätze ins Feld zu führen, die nicht zwangsläufig oder nicht ausschließlich an einen isolierten Träger gekoppelt seien oder gar nicht erst im Kraftfahrzeug, sondern vielmehr direkt auf externen Servern gespeichert würden. Auf letztere sei die Vorschrift des § 903 BGB nicht anwendbar. Vielmehr sei für diese Fälle eine Zuordnung über die Schutzvorschriften des Urheberrechts, des Datenschutzrechts und der gewerblichen Schutzrechte vorzunehmen.

Insoweit ist aufgrund der bestehenden Rechtslage und Rechtsprechung davon auszugehen, dass kein Eigentum an Daten bestehen kann. Somit muss eine Zuordnung von Daten und eine damit einhergehende Befugnis zur Nutzung und Verwendung von Daten über andere rechtliche Vorschriften generiert werden. Es könnte hier vertreten werden, Daten als eigentumsähnliche Position einzustufen mit der Folge, dass die für Eigentum und Besitz geltenden Vorschriften des Bürgerlichen Gesetzbuches angewendet werden könnten und daraus sodann eine Schutzposition abzuleiten wäre.

---

595 Vgl. *Redeker*, NJW 1992, S. 1739–1740 (1739); *Junker*, NJW 1993, S. 824–832 (830).

596 Bundesgerichtshof, Urteil vom 04.11.1987, Aktenzeichen VIII ZR 314/86, NJW 1988, S. 406-410 (408); Bundesgerichtshof, Urteil vom 14.07.1993, Aktenzeichen VIII ZR 147/92, NJW 1993, S. 2436-2439(2437 f.); Bundesgerichtshof, Urteil vom 18.10.1989, Aktenzeichen VIII ZR 325/88, NJW 1990, S. 320-322 (321).

597 Vgl. http://www.uni-muenster.de/Jura.itm/hoeren/materialien/Symposium_Zusammenfassung.pdf.

a) Sachenrecht

Innerhalb des Sachenrechts könnten sich Schutzvorschriften aus den Rechtspositionen des Besitzes und des Eigentums ergeben. Es sei vorweggenommen, dass es nach Ansicht der Bundesregierung[598] kein Eigentum an Daten geben soll. Dieser pauschalen Haltung muss hier nachgegangen werden.

Besitz ist zunächst die vom Verkehr anerkannte tatsächliche Herrschaft einer Person über eine Sache und stellt somit ein tatsächliches Verhältnis und gerade kein subjektives Recht dar.[599]

Im Rahmen eines Kaufvertrages besteht für den Verkäufer die Verpflichtung, den Kaufgegenstand an den Käufer zu übergeben und ihm dadurch den unmittelbaren[600] Besitz zu verschaffen. Insoweit ist davon auszugehen, dass in den vorgenannten Konstellationen jeweils der Käufer als Besitzer anzusehen ist.

Dies könnte auch für die aus dem vernetzten Fahrzeug zu erzeugenden Daten gelten. Es ist allerdings darauf hinzuweisen, dass der Besitz als dingliches Recht nicht an den Daten an sich, sondern allenfalls an dem die Daten speichernden Datenträger bestehen kann. Aufgrund der Tatsache, dass die Daten nichtkörperliche Gegenstände sind, sind an ihnen keine dinglichen Rechte begründbar. Mithin kann über einen etwaigen Besitz am Datenträger aus dem Kraftfahrzeug keine Befugnis abgeleitet werden, über die anfallenden Daten frei und einem Eigentümer gleich zu verfügen.

---

598 BT-Drs. 18/1362 vom 02.05.2014, S. 3, http://dipbt.bundestag.de/dip21/btd/18/013/1801362.pdf.

599 Vgl. *Bassenge* in Palandt/Bassenge: BGB-Kommentar, [74]2015, Überbl v § 854, Rn. 1.

600 Im Zusammenhang mit dem Verkauf eines Kraftfahrzeuges besteht jedoch oftmals die Besonderheit, dass der Verkäufer mittelbarer Besitzer bleibt, indem er sich ein Besitzrecht an dem Kraftfahrzeug vorbehält. Dies ist auch im Hinblick auf einzelne Teile, wie z.B. das OBD-System möglich, vgl. *Roßnagel*, SVR 2014, S. 281–287 (282). Für diese Fälle ist jedoch eine ausdrückliche vertragliche Regelung zu fordern. Dem Verkäufer als mittelbarem Besitzer wird nach der herrschenden Meinung zwar ebenfalls die tatsächliche Sachherrschaft neben dem Käufer als unmittelbarem Besitzer zugesprochen, vgl. nur Bundesgerichtshof, Urteil vom 19.01.1955, Aktenzeichen IV ZR 135/54, in: NJW 1955, S. 499. Als sog. gelockerte Sachherrschaft vermittelt der Käufer dem Verkäufer den Besitz, vgl. *Joost* in Säcker/Rixecker/Oetker: MüKo BGB, Band 6, [6]2013, § 868, Rn. 4. Allerdings dürfte eine solche Konstellation nicht dem Willen des Käufers entsprechen. Nur im Falle eines Kaufvertrages unter Eigentumsvorbehalt und beim Leasingvertrag mittelt der Käufer dem Verkäufer tatsächlich den Besitz. Es besteht jedoch für den Verkäufer nur dann ein Herausgaberecht, wenn der Käufer in Zahlungsverzug gerät oder eine sonstige Pflichtverletzung begeht, indem er z.B. das Kraftfahrzeug als Kaufgegenstand pflichtwidrig weiterveräußert oder es unsachgemäß behandelt, sodass der Verkäufer aus diesem Grund zum Rücktritt berechtigt wäre und dadurch das dem Käufer zustehende Recht zum Besitz nach § 986 BGB beseitigen könnte, vgl. *Weidenkaff* in Palandt/Bassenge: BGB-Kommentar, [74]2015, § 449, Rn. 26..

Als weiteres dingliches Recht zur Begründung einer Zugriffs- und Verfügungsbefugnis über die Daten ist hier das Eigentumsrecht anzuführen. Das Eigentum geht über die sich aus dem Besitz ergebenden Rechte hinaus. Dem Eigentümer einer Sache steht gemäß § 903 Satz 1 BGB das Recht zu, mit der Sache nach Belieben zu verfahren und andere von jeder Einwirkung auszuschließen.[601] Im Rahmen eines Kaufvertrages verpflichtet sich der Verkäufer, dem Käufer grundsätzlich nach § 433 Abs. 2 BGB das Eigentum an der Kaufsache, hier an dem Kraftfahrzeug, zu verschaffen. Geht man von dem Fall aus, dass der Käufer das alleinige Eigentum an dem Kraftfahrzeug erwirbt, wäre es allenfalls durch ausdrückliche vertragliche Vereinbarung möglich, dass sich der Verkäufer ein Sondereigentum an einzelnen Gegenständen, wie z.B. Datenträgern aus dem Kraftfahrzeug erhält. Aber selbst ein solches würde für den Verkäufer ohne gleichzeitige Erfüllung eines Erlaubnistatbestandes aus dem Bundesdatenschutzgesetz kein Recht begründen, beispielsweise aus dem Datenträger personenbezogene Daten abzurufen.[602] Das etwaige Eigentum an dem Datenträger rechtfertigt somit nicht einen Zugriff auf die darauf befindlichen Daten.

Insoweit kann festgestellt werden, dass die dinglichen Rechte des Besitzes und des Eigentums nicht geeignet sind, Zugriffsbefugnisse auf die Daten zu generieren, die sich auf den Datenträgern befinden. An den Daten selbst kann weder Besitz noch Eigentum begründet werden. Aber auch dingliche Rechte an körperlichen Gegenständen wie z.B. den Datenträgern helfen insoweit nicht weiter. Zwar besteht die Möglichkeit, beim Verkauf eines Kraftfahrzeuges in bestimmten Konstellationen Besitz- und Eigentumsrechte sowohl dem Käufer als auch dem Verkäufer zuzuordnen. Aus den Rechten an körperlichen Gegenständen können eben keine Rechte an damit verbundenen nichtkörperlichen Gegenständen abgeleitet werden.

Eine dingliche bzw. sachenrechtliche Zuordnung ist also zwar in Bezug auf das Kraftfahrzeug und darin befindliche Datenträger möglich. Eine Ausweitung dieser Rechte auf Daten an sich gelingt jedoch letztlich nicht.

b) Vertragsrecht

Ein weiterer Ansatzpunkt zur Begründung eigentumsähnlicher Rechte an Daten könnte sich aus den Vorschriften des Vertragsrechts ergeben. Wie soeben festgestellt, spielen

601 Vgl. *Säcker* in Säcker/Rixecker/Oetker: MüKo BGB, Band 6, [6]2013, § 903, Rn. 5.
602 Vgl. *Roßnagel*, SVR 2014, S. 281–287 (283).

vertragliche Vereinbarungen beim (Ver-)Kauf eines Kraftfahrzeugs eine tragende Rolle, um daraus Besitz- oder Eigentumsrechte ableiten zu können. Hierbei besteht jedoch zunächst die Problematik, dass vertragliche Regelungen schuldrechtlich gesehen nur relativ wirken, d.h. lediglich zwischen den Parteien des Kaufvertrages.[603] Die schuldrechtlichen Rechtsverhältnisse stellen hier die Grenzen für etwaige vertragliche Vereinbarungen dar. Darüber hinaus sind jeweils gesonderte Vereinbarungen erforderlich.

Praktisch relevant ist beispielsweise insbesondere eine vertragliche Vereinbarung zwischen Verkäufer und Käufer dahingehend, dass der Händler unentgeltlich Zugriff auf die im Fahrzeug anfallenden Daten und damit Zugang zu diesen haben soll, was als Gefälligkeitsverhältnis bzw. Gefälligkeitsvertrag einzustufen ist und vor allem hinsichtlich nützlicher Aspekte, wie der Fernwartung auch im Interesse des Käufers sein kann.[604] Ihm können dadurch auch weitere Informationen zugänglich gemacht werden. So wäre es dadurch möglich, dem Halter als Kunden bei Wartungsbedarf dies während der Fahrt mitzuteilen und eventuell sogar Terminvorschläge zu unterbreiten.[605]

Allerdings müsste eine solche vertragliche Vereinbarung letztlich zumindest im Hinblick auf personenbezogene Daten auch an den Erlaubnistatbeständen des Datenschutzrechts gemessen werden. Die vertragliche Vereinbarung allein rechtfertigt es an sich nicht, eine eigentümerähnliche Stellung des Händlers als Verkäufer anzunehmen.

Eine Zuordnung von Daten könnte sich im vertragsrechtlichen Bereich letztlich aus den im Zusammenhang mit dem Abschluss eines Kaufvertrages dem Käufer zur Verfügung gestellten AGB ergeben. Grundsätzlich ist dabei zunächst Voraussetzung, dass die AGB als solche im Sinne des Bürgerlichen Gesetzbuches einzustufen sind, wirksam in den Vertrag einbezogen wurden und keine überraschenden Klauseln darstellen.[606] Sofern die vorgenannten Voraussetzungen erfüllt sind, sind die AGB prinzipiell im Wege der Inhaltskontrolle nach §§ 307 bis 309 BGB auf ihre rechtliche Wirksamkeit hin zu prüfen. Etwas anderes gilt für Leistungsbeschreibungen, die Art, Umfang und Güte der Haupt-

603 Vgl. *Mansel* in Jauernig: BGB, [15]2014, § 241, Rn. 4.
604 Vgl. *Roßnagel*, SVR 2014, S. 281–287 (283).
605 Vgl. unter *Kapitel 2, Teil 4, II.4.* und *Kapitel 2, Teil 5, II.*.
606 Die Legaldefinition des Begriffs der allgemeinen Geschäftsbedingungen findet sich in § 305 Abs. 1 Satz 1 BGB. Diese sind wirksam in den Vertrag mit einbezogen, wenn die in § 305 Abs. 2 BGB aufgestellten Voraussetzungen erfüllt sind, der Käufer als andere Vertragspartei also bei Vertragsschluss ausdrücklich auf die AGB hingewiesen und ihm die Möglichkeit gegeben wurde, davon Kenntnis zu erhalten und er auch mit der Geltung derselben einverstanden ist. Überraschende Klauseln im Sinne des § 305c Abs. 1 BGB sind solche, die so ungewöhnlich sind, dass der Käufer als Vertragspartner des Verwenders nicht mit ihnen zu rechnen braucht.

leistung unmittelbar festlegen.[607] Diese unterfallen gerade nicht der Inhaltskontrolle. Aus Gründen der Vertragsfreiheit unterliegen deshalb Abreden unmittelbar über den Gegenstand des Vertrages nicht der Inhaltskontrolle. Auch darunter fallen im Zusammenhang mit dem Kauf von Kraftfahrzeugen etwa die genaue Festlegung von Service- und Wartungsleistungen samt dem dazu erforderlichen vorherigen Datenzugriff.[608] Sollten also Regelungen über einen etwaigen Datenzugriff zur Bereitstellung von Service- und Wartungsleistungen in Gestalt von AGB vorliegen, ist dies möglich und erfordert keine Inhaltskontrolle der Bestimmungen in den AGB.

Durch den Zugriff auf die Daten erlangt der Händler allerdings nicht die Befugnis, den Halter aufgrund vertraglicher Vereinbarung oder aufgrund der Verwendung von AGB von jeder Einwirkung auszuschließen.

c) Strafrecht

Im Bereich der Vorschriften des Strafrechts könnte eine Zuordnung über den Straftatbestand des § 202a StGB erreicht werden. Danach ist der Zugang zu Daten nur dem erlaubt, für den sie bestimmt sind. Hier kommt es wesentlich auf den erlaubten Zugang an. Dies richtet sich in der vorliegenden Diskussion nach der technischen Ausgestaltung der Datenverwendung im Kraftfahrzeug und nach dem Zweck, der hinter der Datenverwendung steht.

Zunächst ist festzustellen, dass alle aus dem Kraftfahrzeug zu generierenden Daten unter den Tatbestand des § 202a StGB zu subsumieren sind.[609]

Vorauszusetzen ist weiterhin die fehlende Verfügungsberechtigung – in der vorliegenden Konstellation der Verwendung von Daten aus vernetzten Dienstfahrzeugen seitens des Arbeitgebers. Die Daten dürfen nicht für ihn bestimmt sein. Es besteht insoweit Einigkeit darüber, dass die Verfügungsberechtigung nicht vom Eigentum am Datenträ-

---

607 Bundesgerichtshof, Urteil vom 12.03.2014, Aktenzeichen IV ZR 295/13, NJW 2014, S. 1658-1663 (1660); Bundesgerichtshof, Urteil vom 09.04.2014, Aktenzeichen VIII ZR 404/12, NJW 2014, S. 2269-2275 (2272).

608 So *Roßnagel*, SVR 2014, S. 281–287 (283).

609 Nach der Legaldefinition des § 202a Abs. 2 StGB sind Daten in diesem Sinne nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden. Die auf Datenträgern gespeicherten Informationen fallen unstreitig unter diesen Datenbegriff, vgl. *Lenckner/Eisele* in Schönke/Schröder: Strafgesetzbuch, [29] 2014, § 202a, Rn. 6. Es muss dabei kein Personenbezug bestehen, vgl. *Weißgerber*, NZA 2003, S. 1005–1009 (1007).

ger abhängt.[610] Dies wird jedoch ein Arbeitgeber regelmäßig einwenden mit der Begründung, dass er als Eigentümer des vom Arbeitnehmer genutzten Speichermediums auch das Recht habe, die darauf gespeicherten Daten abzurufen.[611] Dies lässt sich auch auf solche Fälle übertragen, in denen dem Arbeitnehmer ein im Eigentum des Arbeitgebers stehendes Kraftfahrzeug überlassen wird und der Arbeitgeber die Ansicht vertritt, die in den Steuergeräten des Kraftfahrzeugs gespeicherten Daten stünden in seinem Eigentum, weil das Steuergerät ebenfalls als Bestandteil des Kraftfahrzeugs seinem Eigentum zuzuordnen sei.

Hierbei allerdings eine Verfügungsbefugnis allein vom Eigentum am Datenträger ableiten zu wollen, greift zu weit. Dies insbesondere aufgrund des Aspektes der immer weiter voranschreitenden Vernetzung. Es ist nicht mehr eindeutig feststellbar, an welchem Ort sich die Daten genau befinden, weil sie nicht mehr zweifelsfrei lokalisiert werden können. Noch dazu ist es oftmals der Fall, dass der Eigentümer des Datenträgers gar nicht in näherer Beziehung zu den Daten steht, als dass er Dritten nur den Speicherplatz zur Verfügung stellt.[612] Ebenso kann darauf nicht zurückgegriffen werden, wenn die Daten lediglich übermittelt oder übertragen werden ohne auf einem Datenträger gespeichert zu werden.

Aus vorgenannten Gründen kann es somit nicht lediglich auf das Eigentum am Datenträger ankommen, um daraus eine Verfügungsberechtigung ableiten zu wollen.

Eindeutiger kann die Verfügungsbefugnis über das Merkmal der Erstabspeicherung, des sog. Skripturaktes hergeleitet werden. Danach entsteht die Berechtigung mit der Erstabspeicherung.[613] Dann würde sich eine klare Zuordnung ergeben. Alternativ könnte es jedoch auch auf jede förderliche Beteiligung ankommen, sodass im Ergebnis die Verfügungsbefugnis jedem zuzusprechen sein könnte, der an der Speicherung, Erstellung und Bearbeitung von Daten beteiligt war.[614] Im Ergebnis versagt somit auch hier eine Anlehnung an das Kriterium des Eigentums. Für die Zuordnung ist wiederum auf andere Aspekte abzustellen.

---

610 Vgl. *Fischer*: Strafgesetzbuch, [61]2014, § 202a, Rn. 7a.
611 So *Weißgerber*, NZA 2003, S. 1005–1009 (1007).
612 Vgl. *Hoeren*, MMR 2013, S. 486–491 (487).
613 Vgl. *Fischer*: Strafgesetzbuch, [61]2014, § 202a, Rn. 7a.
614 Vgl. *Weißgerber*, NZA 2003, S. 1005–1009 (1008).

d) Urheberrecht

Auch im Urheberrecht finden sich die aus § 903 BGB im Zusammenhang mit dem Eigentum stehenden Wirkungen. Das Urheberrecht vermittelt einen positiven Inhalt dahingehend, dass nur der Urheber die Verfügungsbefugnis hat und ebenfalls auch einen negativen Inhalt dergestalt, dass einem unberechtigten Dritten diese Befugnis nicht zusteht.[615] Insofern könnte auch über das Urheberrecht ein Schutzmechanismus für Daten aus dem Kraftfahrzeug zur Verfügung stehen.

Für eine etwaige Anwendung der Grundsätze des Urheberrechtsschutzes ist zunächst erforderlich, dass die Daten als solche als Schutzgegenstand und Rechtssubjekt im Sinne des Urheberrechtsgesetzes anzusehen sind. Nach § 2 Abs. 2 UrhG muss es sich um Werke persönlicher geistiger Schöpfung handeln. Es muss dazu eine persönliche Schöpfung vorliegen. Dies meint eine persönliche Leistung, also ein durch einen Menschen geschaffenes und auf dessen Einfall basierendes Werk.[616]

Ungeachtet dessen muss in jedem Fall zusätzlich das Merkmal der geistigen Schöpfung hinzutreten, welches im vorliegenden Zusammenhang problematisch erscheint. Das erforderliche Maß an Schöpfungshöhe wird nur durch denjenigen erreicht, der aus der Masse des Alltäglichen etwas Herausragendes und Besonderes hervorbringt.[617] Es kommt also bei diesem quantitativen Merkmal auf den Grad der Individualität an, an welchen wegen der umfangreichen Befugnisse des Urhebers und der langen Schutzdauer nicht zu geringe Anforderungen zu stellen sind.[618]

In der vorliegenden Diskussion ist jedoch letztlich festzustellen, dass die Daten aus dem Kraftfahrzeug nicht die erforderliche Schöpfungshöhe erreichen, um hier Schutz- und Nutzungsrechte aus dem Urheberrecht auszulösen. Es fehlt sämtlichen Daten an der Kreativität, die im Hinblick auf den Schöpfungsprozess gefordert wird. Dies gilt unabhängig davon, ob es sich um reine Messdaten oder Daten aus Big Data-Anwendungen handelt, die Personenbezug aufweisen. Denn selbst bei der Anwendung von Big Data werden lediglich Programme angewendet, die letztlich die Daten auswerten und neue Daten generieren. Ein menschlicher Gestaltungsprozess liegt dem jedoch nicht zugrun-

615 Vgl. *Eisenmann*: Grundriss Gewerblicher Rechtsschutz und Urheberrecht, [9]2012, Rn. 5.

616 Demnach fallen bereits vorgefundene Gegenstände (sog. Objet trouvé) und alltägliche Gegenstände (sog. Ready-mades) aus dem Anwendungsbereich heraus, vgl. *Wöhrn* in Wandtke: Urheberrecht, [4]2014, 2. Kapitel, Rn. 2.

617 Vgl. *Eisenmann*: Grundriss Gewerblicher Rechtsschutz und Urheberrecht, [9]2012, Rn. 21.

618 Vgl. *Bullinger* in Wandtke/Bullinger: Praxiskommentar zum Urheberrecht, [4]2014, § 2, Rn. 23 f..

de. Auch wird dadurch keine gedankliche oder emotionale Botschaft vermittelt, die auf eine geistige Schöpfung schließen lassen könnte. Ein geistiger und auf den Werkrezipienten zurückzuführender Inhalt lässt sich nicht feststellen. Es handelt sich vielmehr um rein technische Prozesse, die dazu führen, dass Daten aus den Sensoren hergeleitet werden. Darin liegt keine Kreativität. Lediglich für die der Datenverwendung zugrundeliegende Software einer Anwendung handelt es sich aufgrund des niedrigeren Schutzniveaus um eine geistige Schöpfung.[619] Dies ist jedoch nicht auf Daten aus Big Data-Anwendungen zu übertragen. Diese mögen zur Datenerhebung die Nutzung einer Software bedingen. Als Ergebnis zumeist automatisierter Vorgänge wird die geforderte Schöpfungshöhe jedoch nicht erreicht.

Schutz- und Nutzungsrechte könnten sich aber aus spezielleren Vorschriften des Urheberrechts ergeben.

In Betracht könnte ein Schutz über den sog. Erschöpfungsgrundsatz nach § 69c Nr. 3 Satz 2 UrhG kommen.[620] Aber auch hier ist es Voraussetzung, dass eine gewisse Schöpfungshöhe erreicht wird. Dies ist jedoch wie bereits gezeigt bei den Daten aus dem Kraftfahrzeug nicht der Fall.

Weiterhin finden sich Schutz- und Nutzungsrechte des Inhabers der Daten lediglich in § 87a UrhG für den Datenbankhersteller. Das Vorliegen einer Datenbank wird dabei davon abhängig gemacht, dass die Beschaffung, Überprüfung oder Darstellung der Sammlung von Werken eine nach Art oder Umfang wesentliche Investition erfordert. Die Investition muss sich auf die Erstellung der Datenbank als solche beziehen und ist nicht in solchen Mitteln zu sehen, die erst aufgewendet werden müssen, um die Elemente zu erzeugen, aus denen der Inhalt der Datenbank besteht.[621] Eine Investition in die Technik allein ist demnach nicht ausreichend. Bei vernetzten Fahrzeugen und der diesbezüglichen Datengewinnung wird jedoch gerade nicht in die Daten investiert, sondern vielmehr in die Technik, um durch deren Verbesserung noch mehr Daten gewinnen und auswerten zu können. Die Technik ist hier allerdings erst erforderlich, damit überhaupt Daten ermittelt und zusammengestellt werden können. Dies reicht nicht aus, um den

---

619 Das niedrige Niveau der Software zur Einstufung als eigene geistige Schöpfung ergibt sich aus den gesetzlichen Regelungen des § 69a Abs. 3 UrhG bzw. Art 1 Abs. 3 der Richtlinie 2009/24/EG des Europäischen Parlaments und des Rates vom 23.04.2009 über den Rechtsschutz von Computerprogrammen, vgl. *Zech*, CR 2015, S. 137 - 146 (141).

620 Danach erschöpft sich das Recht des Urhebers auf Verbreitung bei Veräußerung eines Vervielfältigungsstückes eines Computerprogrammes.

621 Vgl. *Haberstumpf* in Büscher/Dittmer/Schiwy: Urheberrecht, [3]2015, § 87a, Rn. 9.

Anwendungsbereich des Datenbankschutzes zu eröffnen. Eine Herleitung von Schutz- und Nutzungsrechten scheidet demnach auch hier aus.

Im Bereich des vom Datenbankschutz abzugrenzenden Datenbankwerkschutzes nach § 4 Abs. 2 UrhG muss wiederum festgestellt werden, dass die auch dafür erforderliche Schöpfungshöhe nicht erreicht ist.

Auch hinsichtlich des Schutzes von Lichtbildern nach § 72 UrhG kann keine Zuordnung getroffen werden. Denn dabei wird von dem Speichernden die nach § 2 Abs. 2 UrhG erforderliche Schöpfungshöhe nicht erreicht.

Auch über den Urheberrechtsschutz kann somit keine eigentümerähnliche Stellung hergeleitet werden.

e) Datenschutzrecht

Zuletzt könnte sich eine Zugriffsbefugnis auf Daten aus dem vernetzten Fahrzeug aus dem Datenschutzrecht ableiten. Das Datenschutzrecht betrachtet die Zuordnung von Daten unabhängig von vertraglichen Vereinbarungen oder Besitz- und Eigentumsordnungen. Es wird vielmehr auf eine eigene Informations- und Kommunikationsordnung abgestellt, die darüber zu entscheiden hat, wer wem gegenüber zur Datenverwendung befugt ist.[622] Insoweit kann an dieser Stelle auf sämtliche vorgenannten Erwägungen hinsichtlich des Anwendungsbereichs und der Erlaubnistatbestände des Bundesdatenschutzgesetzes verwiesen werden.[623] Solange also der Anwendungsbereich des Bundesdatenschutzgesetzes eröffnet ist und für die verantwortliche Stelle ein Erlaubnistatbestand greift oder aber der Betroffene in die Datenverwendung eingewilligt hat, können daraus Schutz- und Nutzungsrechte abgeleitet werden.

Auch hierbei sind wiederum die spezialgesetzlichen Vorschriften des Intelligente Verkehrssysteme Gesetz zu beachten, die die Vorschriften des Bundesdatenschutzgesetzes modifizieren.[624]

---

622 So *Roßnagel*, SVR 2014, S. 281–287(283).

623 Vgl. unter *Kapitel 3, Teil 2* sowie *Kapitel 3, Teil 3*.

624 In diesem Zusammenhang ist insbesondere nochmals festzustellen, dass die Datenverarbeitung im Anwendungsbereich des Intelligente Verkehrssysteme Gesetz ebenfalls auf einer Einwilligung des Betroffenen beruhen darf, vgl. hierzu insgesamt unter *Kapitel 3, Teil 3, I.2.b)*.

f) Zwischenergebnis

Obgleich man ein Eigentum an Daten in sachenrechtlicher Hinsicht verneint, ist zu beachten, dass trotzdem keine freie Nutzung möglich ist. Eine solche wird beschränkt durch die Vorgaben des Bundesdatenschutzgesetzes. Jedoch sollte nach *Duisberg* der Versuch unternommen werden, jemandem eine primäre Zuständigkeit über die Daten zuzuordnen.[625] Dies lässt sich letztlich auch ohne Schaffung von Dateneigentum anhand der vorgenannten Vorschriften verschiedener Rechtsbereiche in den Griff bekommen. Die Erlaubnis der Verwendung von Daten sollte daran gemessen werden, ob diese jemandem rechtlich zuzuordnen sind. Dies muss sich insbesondere am Datenschutzrecht messen lassen. Damit können alle zu berücksichtigenden Interessen in Einklang gebracht werden. Einer Begründung zivilrechtlichen Dateneigentums im Sinne eines originären Ausschließlichkeitsrechts müsste allerdings im Wege der richterlichen Rechtsfortbildung begegnet werden, wofür bislang keine hinreichenden gesetzlichen Grundlagen bestehen.[626]

Insoweit sind die personenbezogenen Daten aus vernetzten Fahrzeugen über die vorgenannten Schutzmechanismen abzusichern.

2. Faktische Herrschaftsposition bei rechtlich freien Daten

Unabhängig von der Frage nach dem Eigentum an Daten und einem rechtlichen Schutz derer könnte aber auch eine faktische Herrschaftsposition hinsichtlich solcher Daten bestehen, die rechtlich *„frei“* sind, also nach Maßgabe des Bundesdatenschutzgesetzes und anderer Schutzrechte niemandem ausschließlich zugeordnet werden können. Hierunter fallen die nicht-personenbezogenen Daten. Aus einer solchen faktischen Herrschaftsposition könnten sich wiederum Rechte ableiten lassen.

Dies wird insbesondere im Hinblick auf den Zugang zu Reparatur- und Wartungsinformationen als nicht personenbezogene Daten relevant. Auch wenn es sich bei diesen Daten lediglich um technische Daten handelt, die grundsätzlich keinen Personenbezug aufweisen, sind diese für Versicherer, Arbeitgeber, Autobanken etc. wertlos, wenn kein tatsächlicher Zugriff auf die Daten besteht.

---

625 Vgl. http://www.car-it.com/rechtsfreier-raum-wem-gehoeren-die-daten-aus-dem-auto/id-0039081.
626 Vgl. *Dorner*, CR 2014, S. 617-628 (626).

a) Datenmonopol

Dies ist beispielsweise der Fall, wenn Hersteller die Schnittstellen in den Fahrzeugen derart verschlüsseln, dass Werkstätten oder auch Versicherer darauf nicht zugreifen können. Insoweit könnte dadurch ein Datenmonopol der Autohersteller über Fahrzeugdaten hinsichtlich Wartung und Nutzung der Fahrzeuge entstehen. Aber auch der Fahrzeughalter besitzt weder die Geräte, um die technischen Daten auszulesen, noch das Fachwissen, um diese technisch zu verstehen und daraus eventuell Rückschlüsse zu ziehen, sodass die Daten auch für ihn mangels technischer Komponente und notwendigem Wissen nutzlos sind.[627] Noch dazu besteht die Gefahr, dass die Fahrer zukünftig tiefer in die Tasche greifen müssen, wenn sie wegen der Monopolstellung der Hersteller und der mit diesen verbundenen Vertragswerkstätten nach dem Kauf des Kraftfahrzeuges auf die eventuell kostspieligere Reparatur in der Vertragswerkstatt angewiesen sind.[628]

Es stellt sich also die Frage, wie mit einer solchen faktischen Herrschaftsposition der Hersteller und Vertragswerkstätten umzugehen ist und einem möglichen Datenmonopol der Hersteller entgegengewirkt werden kann.

Zunächst ist festzustellen, inwieweit bereits ein Datenmonopol der Hersteller und Vertragswerkstätten besteht und welche Entwicklung dies durch die Vernetzung von Kraftfahrzeugen nehmen wird. Die Diskussion um ein Datenmonopol der Kraftfahrzeughersteller kommt insbesondere in Bezug auf die verpflichtende Einführung des sog. e-Calls[629] auf. Es besteht dabei die Möglichkeit, neben der verpflichtenden Integration des eCall-Notrufsystems das sog. Service Call-System (sCall) zu nutzen, welches dem Fahrer zusätzliche Dienstleistungen anbietet und beispielsweise im Falle eines Unfalls automatisch zusätzlich den Abschleppdienst der Vertragswerkstatt informiert.[630] Die Autofahrer könnten dabei allerdings nur die Dienste nutzen, die vom jeweiligen Autohersteller angeboten werden.[631]

Aber auch im Zusammenhang mit Reparatur- und Wartungsarbeiten am Kraftfahrzeug wird ein möglicher Datenvorsprung der Hersteller relevant. Aufgrund der immer weiter

---

627 Vgl. http://www.delegedata.de/2014/05/datenschutz-im-auto-bundesregierung-hoechst-komplex/.
628 Vgl. http://www.goslar-institut.de/.
629 Vgl. unter *Kapitel 2, Teil 5, III.*.
630 Vgl. *Schinhammer*, Autohaus 2012, S. 96–97 (96).
631 Vgl. http://www.gdv.de/2014/10/ecall-warnung-vor-datenmonopol-der-autohersteller/.

voranschreitenden technischen Entwicklung und des sich erhöhenden Anteils an Sensoren und Steuergeräten im Kraftfahrzeug ist es schon jetzt erforderlich, im Rahmen von Wartungs- und Verschleißarbeiten auf die technischen Informationen zu jedem einzelnen Kraftfahrzeugmodell zugreifen zu können. Dies gestaltet sich jedoch schwierig. Meist fehlen in Benutzerhandbüchern der Kraftfahrzeuge wichtige Hinweise z. B. zur Elektrik und werden auch von Herstellern nicht in gedruckter Form zur Verfügung gestellt mit der Folge, dass der Halter bei Problemen auf die Hilfe von Werkstätten dringend angewiesen ist.[632] Die Modelle unterscheiden sich heute bereits derart, dass eine allgemeinverbindliche Information nicht existiert und somit auch nicht ausreichen kann, um eine Reparatur ordnungsgemäß durchzuführen. Eine in der Vergangenheit wenig komplexe Tätigkeiten, wie z.B. der Austausch einer beschädigten Windschutzscheibe, kann bei aktuellen und mit einem Regensensor oder verbauter Kameratechnik ausgestatteten Kraftfahrzeugmodellen nicht mehr ohne Reparatur- und Wartungsinformationen bzw. ohne Diagnose-Systeme fachgerecht durchgeführt werden.[633]

Dies zeigt bereits jetzt das Ausmaß an Komplexität hinsichtlich der Technik in Kraftfahrzeugen. Freie Werkstätten könnten also ohne die erforderlichen Informationen in naher Zukunft nicht mehr in der Lage sein, selbst die Reparatur- und Wartungsarbeiten anzubieten. Dadurch würde ihnen der Zugang zum Reparaturmarkt wesentlich erschwert. Dies stellte sich als Eingriff in die tagtäglichen Prozesse der freien Werkstätten und sonstigen Dienstleister dar und würde zum Ende des Wettbewerbs zwischen Vertragswerkstätten und freien Werkstätten führen. Denkbar wäre ebenfalls, dass durch diese Handhabe auch unabhängige Prüforganisationen im Verkehrsbereich, wie z.B. die DEKRA, keinen Zugriff mehr auf die erforderlichen Informationen hätten und dadurch letztlich das Sicherheitsniveau auf deutschen Straßen gefährdet würde. Auch das Europäische Parlament hat sich im Zusammenhang mit dem verpflichtenden Einbau des e-Call-Systems für eine diskriminierungsfrei zugängliche Schnittstelle ausgesprochen.[634] Es muss auch Fahrern, Haltern, Versicherern, Autobanken und insbesondere den freien Werkstätten möglich sein, über eine Schnittstelle Zugriff auf die für Reparatur und Wartung relevanten Daten zu erhalten.

---

632 So ist es bei Modellen von Volkswagen erforderlich, sich auf einer Website einzuloggen und für die Nutzung eine stündliche Gebühr von 5,- € zu zahlen, um an etwaige Informationen heranzukommen, vgl. ADAC Motorwelt (4/2015), S. 36.

633 Vgl. http://www.k-t-i.de/fileadmin/edit/publikationen/ti/2013/2013-02_TI_Euro-5-6_V1.0.pdf.

634 Vgl. http://www.springerprofessional.de/e-call-als-datenmonopol-fuer-autohersteller/5381860.html.

Insofern sind hier insgesamt verschiedenste Akteure in diese Problematik verwickelt, die insgesamt den Herstellern und freien Werkstätten gegenüberstehen. Die Waffengleichheit im Wettbewerb würde hinfällig, wenn ein Datenmonopol auf Seiten der Hersteller entstehen könnte, ohne dass es für die sonstigen Wettbewerbsteilnehmer eine Möglichkeit geben würde, ebenfalls Anspruch auf die Informationen geltend zu machen.

b) Recht auf Daten nach der EURO 5/6-Verordnung

Um ein solches Datenmonopol zu verhindern, müsste die Frage gestellt werden, ob hier nicht aus dem sog. Typzulassungsrecht ein Recht auf die Daten abgeleitet werden kann. Im Regelungsbereich des eCall-Systems wird durch die bisher vorhandenen Regelungswerke lediglich der automatisierte Notruf reguliert. Sonstige Telematik-Anwendungen und deren rechtliche Einordnung sowie der Umgang im Wettbewerb sind bisher noch keinem regulatorischen Rahmen unterworfen. Relevant ist in diesem Zusammenhang Kapitel III (Art. 6-9) über den Zugang zu Reparatur- und Wartungsinformationen für Fahrzeuge in der sog. EURO 5/6 Verordnung (EURO 5/6-VO)[635].

Nach Art. 6 Abs. 1 EURO 5/6-VO hat der Hersteller unabhängigen Marktteilnehmern[636] über das Internet mithilfe eines standardisierten Formats uneingeschränkten und standardisierten Zugang zu Reparatur- und Wartungsinformationen[637] auf leicht und unverzüglich zugängliche Weise zu gewähren und derart, dass gegenüber dem Zugang der autorisierten Händler und Reparaturbetriebe oder der Informationsbereitstellung für diese keine Diskriminierung stattfindet. Die erforderlichen Informationen umfassen insbesondere die eindeutige Identifizierung des Fahrzeugs, Servicehandbücher, techni-

---

635 *Verordnung (EG) Nr. 715/2007 des Europäischen Parlaments und des Rates vom 20. Juni 2007 über die Typgenehmigung von Kraftfahrzeugen hinsichtlich der Emissionen von leichten Personenkraftwagen und Nutzfahrzeugen (Euro 5 und Euro 6) und über den Zugang zu Reparatur- und Wartungsinformationen für Fahrzeuge vom 29.06.2007*, ABl. Nr. L 171 S. 1.

636 *„Unabhängige Marktteilnehmer"* sind Unternehmen, die keine autorisierten Händler oder Reparaturbetriebe sind und die direkt oder indirekt an der Wartung und Reparatur von Kraftfahrzeugen beteiligt sind, insbesondere Reparaturbetriebe, Hersteller oder Händler von Werkstattausrüstung, Werkzeugen oder Ersatzteilen, Herausgeber von technischen Informationen, Automobilclubs, Pannenhilfedienste, Anbieter von Inspektions- und Prüfdienstleistungen sowie Einrichtungen der Aus- und Weiterbildung von Mechanikern, Herstellern und Reparaturkräften für Ausrüstungen von Fahrzeugen, die mit alternativen Kraftstoffen betrieben werden, vgl. Art. 3 Nr. 15 EURO 5/6-VO.

637 *„Reparatur- und Wartungsinformationen"* sind sämtliche für Diagnose, Instandhaltung, Inspektion, regelmäßige Überwachung, Reparatur, Neuprogrammierung, Neuinitialisierung des Fahrzeugs erforderlichen Informationen, die die Hersteller ihren autorisierten Händlern und Reparaturbetrieben zur Verfügung stellen, einschließlich aller nachfolgenden Ergänzungen und Aktualisierungen dieser Informationen, wobei diese Informationen auch sämtliche Informationen umfassen, die für den Einbau von Teilen oder Ausrüstung in ein Fahrzeug erforderlich sind, vgl. Art. 3 Nr. 14 EURO 5/6-VO.

sche Anleitungen sowie Fehlercodes des Diagnosesystems (einschließlich herstellerspezifischer Codes).[638] Um auch im Nachhinein eine Diskriminierung zu verhindern, muss der Hersteller Änderungen und Ergänzungen seiner Reparatur- und Wartungsinformationen zum selben Zeitpunkt im Internet zugänglich machen, zu dem er diese auch seinen autorisierten Reparaturbetrieben zur Verfügung stellt.[639]

Aber auch im Zusammenhang mit Typgenehmigungsverfahren zur Herstellung neuer Kraftfahrzeuge gibt es Regelungen dahingehend, dass der Hersteller, der für ein Fahrzeug die EG-Typgenehmigung oder die nationale Typgenehmigung beantragt, der Typgenehmigungsbehörde die Einhaltung der EURO 5/6-VO bezüglich des Zugangs zu Reparatur- und Wartungsinformationen nachweisen muss.[640]

Es wird also für freie Werkstätten ein uneingeschränkter und standardisierter Zugang zu technischen Informationen seitens der Hersteller geschuldet.

Unter Anwendung von Wortlaut- und teleologischer Auslegung lässt es sich durchaus vertreten, hier ein Recht auf Daten für unabhängige Marktteilnehmer zu generieren.

Der Wortlaut der einschlägigen Vorschriften der EURO 5/6-VO ist hier eindeutig. Nach Art. 6 Abs. 1 EURO 5/6-VO *„hat“* der Hersteller den unabhängigen Marktteilnehmern den Zugang zu den entsprechenden Informationen zu gewähren. Es handelt sich gerade nicht um eine sog. Soll-Vorschrift. Dem unabhängigen Marktteilnehmer steht folglich ein solcher Anspruch zu.

Auch Sinn und Zweck der Vorschriften und der Verordnung sprechen für eine solche Auslegung der Normen. Denn nach dem Telos der Verordnung soll der diskriminierungsfreie Zugang zu Wartungs- und Reparaturinformationen der Aufrechterhaltung des fairen Binnenmarktes dienen. Ein unbeschränkter Zugang zu den für die Fahrzeugreparatur notwendigen Informationen über ein standardisiertes Format zum Auffinden technischer Informationen und ein wirksamer Wettbewerb auf dem Markt für Fahrzeugreparatur- und -Wartungsinformationsdienste sind für ein besseres Funktionieren des Binnenmarkts notwendig, insbesondere hinsichtlich des freien Warenverkehrs, der Niederlassungsfreiheit und der Dienstleistungsfreiheit.[641] Bei all diesen Aspekten handelt es

638 Vgl. Art. 6 Abs. 2 EURO 5/6-VO.
639 Vgl. Art. 6 Abs. 8 EURO 5/6-VO.
640 Vgl. Art. 6 Abs. 7 EURO 5/6-VO.
641 Vgl. Erwägungsgrund (8) EURO 5/6-VO.

sich um Rechte und Freiheiten, die dem Einzelnen auf europäischer Ebene als Grundfreiheiten zur Seite stehen. Dies zeigt die Bedeutung, die dem diskriminierungsfreien Zugang zu den hier relevanten Informationen beigemessen wird.

Die Auslegung sollte hier so weit gehen, dass sämtliche Informationen, die auch nur mittelbar mit Wartung oder Instandsetzung von Fahrzeugen zu tun haben, auf diskriminierungsfreier Basis dem freien Markt zur Verfügung zu stellen sind. Ein Recht auf diese Daten muss hier angenommen werden. Nur so lassen sich auf lange Sicht die Entstehung eines Datenmonopols und eine damit einhergehende Verzerrung bzw. ein Ende des Wettbewerbs verhindern. Dies und die Gewährung eines freien Binnenmarktes sind Sinn und Zweck der Verordnung und insbesondere des III. Kapitels der EURO 5/6-VO.

Dieser Argumentationslinie entsprechend entschied auch das Landgericht Frankfurt am Main[642]. Die Pflicht des Herstellers aus Art 6 Abs. 1 S. 1 EURO 5/6-VO erschöpfe sich danach nicht in der bloßen Bereitstellung der Informationen über eine Website mit Suchfunktion, sondern verlange die Bereitstellung eines Internetdienstes über definierte Schnittstellen und Formate. Zur Verfügung gestellt werden müssten sämtliche Reparatur- und Wartungsinformationen gemäß Art. 3 Nr. 14 EURO 5/6-VO. Ziel sei die Verhinderung von Diskriminierung auf dem Ersatzteilemarkt.

Einem Datenmonopol muss hier durch umfassende Zugangsgewährung gegen Entgelt entgegengewirkt werden. Die zur Durchsetzung notwendigen Rechte stehen den Betroffenen über die Vorschriften der EURO 5/6-Verordnung zur Verfügung.

III. Schutz vor Daten

Als zweiter Aspekt ist im vorliegenden Kontext auch die Frage nach dem Schutz *„vor“* Daten zu stellen:

„Wie kann der Betroffene vor Daten geschützt werden?“

Diese Frage stellt den eigentlichen Kernbereich des Datenschutzrechtes dar. Daten können für den Betroffenen in vielfältiger Weise gefährlich werden und damit ein Schutzbedürfnis auslösen. Zu denken sei hier beispielsweise an einen „*Angriff*“ von Daten dadurch, dass die erhobenen Daten über Viren oder Trojaner missbraucht werden kön-

642 Landgericht Frankfurt am Main, Urteil vom 21.01.2016, Aktenzeichen 2-03 O 505/13, https://www.telemedicus.info/urteile/Internetrecht/1675-LG-Frankfurt-a.M.-Az-2-03-O-50513-Zugangsanspruch-unabhaengiger-Unternehmen-zu-VIN-Datenbank-KIA.html.

nen und letztlich dazu führen, dass durch eine derartige Verwendung dieser Daten Sicherheitslücken in Systemen des Betroffenen auftreten. Insoweit könnten die Daten, sofern sie in die falschen Hände geraten, sich gegen den Betroffenen richten und für diesen eine Gefahr darstellen. Hacker können durch Sicherheitslücken an Passwörter oder sonstige sensible Daten kommen.

Der notwendige Schutz bezieht sich dabei darauf, von Anfang an so wenige Daten wie möglich überhaupt zu generieren. Hierbei sind insbesondere die Prinzipien der Datensparsamkeit und Datenvermeidung zu beachten.[643]

Es entstehen heutzutage Unmengen an Datensätzen. Problematisch und erschreckend ist dabei jedoch zu bemerken, dass sich die Menschen scheinbar nur beiläufig und nicht im eigentlich notwendigen Maße damit auseinandersetzen, welche Daten sie preisgeben und dass oftmals diese Preisgabe unbewusst und vor allem auch unentgeltlich erfolgt.

Eine Registrierungsmöglichkeit beispielsweise bei Facebook wird den Betroffenen kostenlos offeriert. Dazu müssen sie „*lediglich*“ einige persönliche Angaben machen und ein Profil erstellen. Es wird hierbei den wenigsten tatsächlich klar sein, dass sie für den Zugang zu einem solchen Netzwerk mit ihren eigenen Daten bezahlen. Und auch die Tatsache, dass genau diese Daten später von Facebook selbst zu Werbezwecken oder zum Verkauf an Dritte genutzt werden, scheint den Betroffenen nicht bewusst zu sein.

Doch mit dem Einzug von Facebook & Co. in das Kraftfahrzeug wird dies unmittelbar auch im vernetzten Kraftfahrzeug zu problematisieren sein. Durch die persönlichen Angaben und bei Facebook hinterlegten Interessen kann durch Big Data-Anwendung[644] und Verknüpfung mit den aus dem vernetzten Fahrzeug generierten Daten ein umfassendes Persönlichkeitsprofil erstellt werden. Wenn man sodann bedenkt, dass dies für Facebook, Kraftfahrzeughersteller und sämtliche andere Dritte als Nutzer der Daten nahezu unentgeltlich sein soll, müssten sämtliche Warnsignale ertönen.

Die Betroffenen sind dahingehend zu sensibilisieren, dass ihre Daten insgesamt und auch jedes einzelne Datum einen finanziellen und ökonomischen Wert haben. Gleiches gilt für die Privatsphäre der einzelnen Personen.

---

643 Vgl. unter *Kapitel 3, Teil 2*.
644 Vgl. unter *Kapitel 2, Teil 5*.

1. Ökonomischer Wert von Daten

Datenschutz bedeutet auch Schutz der Privatsphäre. Je weniger Daten einer Person anderen zur Nutzung zur Verfügung stehen, umso mehr kann die Privatsphäre des Einzelnen geschützt werden. Wenn jemand jedoch bereit ist, seine Privatsphäre mit anderen zu teilen und seine Daten zur Verfügung zu stellen, so muss er sich bewusst sein, welcher Wert hinter den Daten steckt und wie er diesbezüglich verhandeln sollte.

a) Monetarisierung der Privatsphäre

In diesem Zusammenhang wird oft der Begriff der *„Monetarisierung der Privatsphäre"* ins Spiel gebracht. Darunter versteht man die Kompensation für den Verzicht auf Privatsphäre, also die Preisgabe von persönlichen Informationen gegen Bezahlung.[645] Dabei sind vor allem die Interessen der verschiedenen am Datenaustausch beteiligten Parteien zu beachten.[646]

Es sei festgestellt, dass es sich bei dem Wert eines Gutes um eine ökonomische Kategorie handelt, die die Grundlage für eine spätere Preisbildung im Wirtschaftsleben darstellt.[647] Der Wert eines Gutes meint seine Bedeutung als Mittel zur Bedürfnisbefriedigung und hängt von Angebot und Nachfrage ab.[648] Zu Beginn des Internetzeitalters war der US-amerikanische Ökonom *Hal Varian* noch der Auffassung, dass es ausreichend sei, wenn ein Verbraucher seine privaten Daten tatsächlich als Eigentum einordnen würde.[649] Dem lag wohl die Beurteilung der Position des Eigentums als tragende Säule der Privatrechte zugrunde. Mit Blick auf die heutige Situation muss diese Einschätzung *Varians* allerdings neutralisiert werden. Dies zeigen vielfältige Studien, die sich mit dem Wert von Daten als Wirtschaftsgut auseinandersetzen. Beispielhaft sei hier auf die Studie des Wissenschaftszentrums Berlin zum Thema *„Unwillingness to Pay for Pri-*

---

645 Vgl. *Jentzsch*, DIW Wochenbericht Nr. 34.2014, S. 793–798 (793).

646 Während für Online-Anbieter ethisch-moralische Aspekte eines Eingriffs in die Privatsphäre des Internetnutzers kein primäres Thema sind, hat der Verbraucher mögliche Vorteile (Prämien und Boni, kostenlose Nutzung von Internetangeboten, Rabattierung von Produkten) und Nachteile (Belästigung mit Werbung Kontrollverlust persönlicher Daten, Gefühl der Beobachtung und Entprivatisierung) gegeneinander abzuwägen und die für ihn beste Strategie zu wählen, vgl. *Hess/Schreiner*, DuD 2012, S. 105–109 (106, 108). Hinzu kommt für ihn die Schwierigkeit, dass ein faires Aushandeln der Gegenleistung ihm aufgrund der ökonomischen und organisatorischen Macht, des technischen und rechtlichen Knowhows sowie der Bestimmungsmöglichkeit hinsichtlich der Vertragsbestimmungen und der Art der Verarbeitung von Seiten der verarbeitenden Stelle nur selten möglich ist, vgl. *Weichert*, NJW 2001, S. 1463–1469 (1466).

647 Vgl. https://de.wikipedia.org/wiki/Wert_(Wirtschaft).

648 Vgl. *Seidel*: Grundlagen der Volkswirtschaftslehre, [21]2003, S. 16.

649 Vgl. http://www.zeit.de/2010/29/Verbraucher-Privatsphaere.

vacy: A Field Experiment" hingewiesen.[650] Das Ergebnis der Studie indiziert eindeutig, dass den Menschen in der heutigen Zeit zwar der Datenschutz an sich wichtig ist, sie aber bereit sind, auf ausreichenden Datenschutz zumindest teilweise zu verzichten, sofern damit finanzielle Vorteile für sie einhergehen.

b) Richtlinie über bestimmte vertragliche Aspekte der Bereitstellung digitaler Inhalte

In diesem Zusammenhang relevant ist der zwischenzeitlich vorliegende Entwurf einer Richtlinie über bestimmte vertragliche Aspekte der Bereitstellung digitaler Inhalte (RL-Bereitstellung-E).[651] Ziel ist die Schaffung vollständig harmonisierter Verbrauchervertragsvorschriften in allen Mitgliedstaaten der Europäischen Union.[652] Nach Art. 3 Nr. 1 RL-Bereitstellung-E soll die Harmonisierung durch die Richtlinie für alle Verträge gelten, auf deren Grundlage ein Anbieter einem Verbraucher digitale Inhalt bereitstellt oder sich hierzu verpflichtet und der Verbraucher als Gegenleistung einen Preis zahlt oder *„aktiv eine andere Gegenleistung als Geld in Form personenbezogener oder anderer Daten erbringt"*. Dies wird damit begründet, dass in der digitalen Wirtschaft Informationen über Einzelpersonen für Marktteilnehmer immer mehr einen mit Geld vergleichbaren Wert haben und deshalb zur Vermeidung von Diskriminierung eine Differenzierung nach Art der Gegenleistung nicht tragbar wäre.[653]

Sollte der Entwurf dieser Richtlinie dergestalt umgesetzt werden, würde dies ausdrücklich die soeben dargestellten Aspekte in einer rechtlichen Grundlage zusammenfassen. Dies könnte zum Erkenntnisgewinn auf Seiten der Verbraucher führen, dass die Bereitstellung von Daten gerade einen geldwerten Vorteil beim Vertragspartner auslöst. Zudem würde die Richtlinie ergänzend neben die Datenschutz-Grundverordnung treten,

---

650 Als Ausgangssituation wurden den Teilnehmern der Studie zwei Onlineshops vorgestellt mit der Maßgabe, bei einem von beiden eine CD zu kaufen. Beide Onlineshops unterschieden sich darin, dass bei Shop Nr. 1 nur gering sensible Daten angegeben werden mussten – nämlich nur das Geburtsjahr und die Lieblingsfarbe –, während bei Shop Nr. 2 sehr sensible Datenangaben zum Monatseinkommen und Geburtsdatum erforderlich waren, die CD allerdings in Shop Nr. 2 einen Euro billiger war. Das Ergebnis überrascht nicht: Fast 92 % der Teilnehmer kauften in Shop Nr. 2. Allerdings betonten gleichzeitig ¾ der Teilnehmer, dass ihnen Datenschutz wichtig sei, vgl. http://ftp.iza.org/dp5017.pdf.

651 *Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte vom 09.12.2015*, COM(2015) 634 final, https://ec.europa.eu/transparency/regdoc/rep/1/2015/DE/1-2015-634-DE-F1-1.PDF.

652 Vgl. Erwägungsgrund (6) RL-Bereitstellung-E.

653 Vgl. Erwägungsgrund (13) RL-Bereitstellung-E.

die eine solche Regelung bislang nicht enthält. Es bleibt abzuwarten, in welcher Gestalt die Richtlinie erlassen wird.

c) Ökonomischer Wert von Daten bei Big Data-Anwendungen

Solche vorgenannten Daten werden insbesondere im Bereich von Big Data-Anwendungen und hierbei gerade auch im vernetzten Fahrzeug einen sehr hohen ökonomischen Wert erreichen, wenn es dadurch möglich wird, einen *„digitalen Zwilling"* einer Person zu erzeugen. Auch dieser Gefahr sind sich viele Verbraucher nicht bewusst, wie auch der Bundespräsident *Joachim Gauck* in einer Rede aus dem Jahr 2013 feststellte:

> *„Sie verstehen nicht oder sie wollen nicht wissen, dass sie so mit bauen an einem digitalen Zwilling ihrer realen Person, der neben ihren Stärken eben auch ihre Schwächen enthüllt – oder enthüllen könnte. Der ihre Misserfolge und Verführbarkeiten aufdecken oder gar sensible Informationen über Krankheiten preisgeben könnte. Der den Einzelnen transparent, kalkulierbar und manipulierbar werden lässt für Dienste und Politik, Kommerz und Arbeitsmarkt."*[654]

Auch im Rahmen von Big Data-Anwendungen hat immer noch jede einzelne Information in einem etwaigen Profil ihren eigenen ökonomischen Wert mit wertvollen Anknüpfungs- und Monetarisierungspunkten für verschiedenste Akteure.[655] Im Bereich des vernetzten Fahrzeugs kommen hierfür der Kraftfahrzeughersteller, der Arbeitgeber, die Versicherungsbranche, Autobanken und viele weitere Dritte in Betracht.

Aufgrund der vorgenannten Aspekte scheint es nicht selbstverständlich zu sein, die eigenen Daten als Wirtschaftsgut anzusehen. Allein die Tatsache, dass Daten mehrmals weitergegeben werden können, lässt Verbraucher deren Exklusivität nicht erkennen. Dass sie mit jeder Datenweitergabe ein Stück Privatsphäre preisgeben, ist den meisten derzeit noch nicht bewusst.

Die Thematik der Monetarisierung der Privatsphäre hat mittlerweile auch auf europäischer Ebene Beachtung gefunden. So befördert die Europäische Kommission mit der sog. *„Horizon-2020-Ausschreibung"* Vorschläge zur Monetarisierung der Privatsphäre

---

654 Vgl. http://www.bundespraesident.de/SharedDocs/Reden/DE/Joachim-Gauck/Reden/2013/10/131003-Tag-deutsche-Einheit.html.

655 Vgl. http://www.dbresearch.de/PROD/DBR_INTERNET_DE-PROD/PROD0000000000328652.PDF.

und hat die Idee entwickelt, der Verbraucher müsse gerechter für die Informationspreisgabe entlohnt werden und im Rahmen der Ausschreibung spezifiziert, dass persönliche Daten zwar mittlerweile als Wirtschaftsgut gehandelt würden, jedoch gerade nicht der Eigentümer, sondern Dritte damit Geld verdienten, die die Daten sammeln.[656] Dies verdeutlicht nochmals den ansteigenden Stellenwert der Problematik.

2. Ausschließbarkeit

Es spielt schließlich auch eine Rolle, dass die Daten nicht abgeschlossen von der Außenwelt nur dem Verbraucher zur Verfügung stehen. Aufgrund der technischen Vernetzung und der dadurch vorhandenen Angebote stellt es sich für Verbraucher immer schwieriger dar, die Daten allein für sich zu behalten und andere komplett von dem Gebrauch der Daten und der daraus zu gewinnenden Informationen auszuschließen. Dies belegen in drastischer Weise auch verschiedenste Datenschutzskandale[657], bei denen Verbraucherdaten scheinbar ohne großen Aufwand beschafft werden konnten. Die Ausschließbarkeit von Daten gegenüber Dritten stellt sich im Zusammenhang mit vernetzten Fahrzeugen gegenüber verschiedenen Akteuren als schwierig dar. Eine Rolle in dem Datengeflecht spielen insbesondere Fahrer, Halter, Hersteller, Dritte als Insassen, Versicherer, Werkstätte, Autobanken, aber auch Drittanbieter, wie z.B. ein kommerzieller Rettungsdienst oder Anbieter von Telemediendiensten.

Die Vielzahl der Akteure wirft jedoch die Frage auf, ob nicht – von dem Extremfall eines Datenschutzskandals oder -missbrauchs abgesehen – doch grundsätzlich eine Ausschließbarkeit gegenüber Dritten geltend gemacht werden kann. Wie bereits festgestellt, besteht kein Eigentum an Daten und auch eine Zuordnung der Daten ist nicht möglich, soweit kein Sonderrechtsschutz besteht.[658] Die Daten dürfen also an sich grundsätzlich uneingeschränkt verwendet werden. Die Nutzung hat jedoch im Rahmen der Gesetze zu erfolgen.

---

656 Vgl. *Jentzsch*, DIW Wochenbericht Nr. 34.2014, S. 793–798 (793, 797). sowie https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-ds-2014-1.html.

657 Beispielhaft sei hier ein Datenschutzskandal bei Apple im Jahr 2014 angeführt. Apple überwachte dabei seine Mitarbeiter in deren Arbeitsbereich im Apple-Store in Hamburg mittels Videokamera. Nachdem das Arbeitsgericht Frankfurt am Main dies für illegal erachtete (Az.: 22 Ca 9428/12), zahlte Apple ein Schmerzensgeld an die Betroffenen in Höhe von 3.500,- € und die Kameras wurden daraufhin so ausgerichtet, dass die Arbeitsplätze nicht mehr direkt überwacht wurden, vgl. http://www.heise.de/newsticker/meldung/Videoueberwachung-Apple-muss-Schmerzensgeld-zahlen-2289537.html.

658 Vgl. unter *Kapitel 3, Teil 4, II.1.*.

Anders stellt sich dies nur für Daten dar, die Personenbezug aufweisen. In diesen Fällen ist gemäß §§ 1 Abs. 1, 4 Abs. 1 BDSG eine abweichende Beurteilung derart vorzunehmen, dass dabei eine Zuordnung durch den Personenbezug hergestellt wird und infolgedessen eine Datenverwendung lediglich aufgrund gesetzlicher Erlaubnis oder aufgrund einer durch den Betroffenen erteilten Einwilligung gerechtfertigt ist. Soweit also personenbezogene Daten betroffen sind, kann bei Überschreiten der gesetzlichen Grenzen also tatsächlich auch eine Ausschließbarkeit hinsichtlich der Daten für Dritte abgeleitet werden.

Das Zusammenspiel der Aspekte der Ausschließbarkeit und der Rivalität ermöglicht eine erste Einschätzung, um welche Art von Gut es sich bei einzelnen Daten handelt. Güter lassen sich anhand dieser Merkmale in verschiedene Gruppen einteilen.[659] Wie bereits festgestellt[660] werden Daten als Wirtschaftsgüter von der Nicht-Ausschließbarkeit und der Nicht-Rivalität beherrscht. Es handelt sich dabei also zunächst um öffentliche Güter, deren Verwendung jedoch im Falle eines vorliegenden Personenbezugs den gesetzlichen Vorschriften des Bundesdatenschutzgesetzes und etwaiger Spezialgesetze unterliegt. Dies trifft mithin auch auf die aus dem vernetzten Fahrzeug zu generierenden Daten zu.

3. Zugriffsbefugnisse des Arbeitgebers

Nachdem festgestellt wurde, dass Daten je nach Personenbezug einer Zugriffsbefugnis des Betroffenen oder der verantwortlichen Stelle unterliegen und demnach Dritte je nach Einzelfall von einer Datenverwendung ausgeschlossen werden können, sind diese

---

659 Bei den sog. öffentlichen Gütern ist weder Ausschließbarkeit noch Rivalität gegeben. Dies sind somit Güter der Allgemeinheit, wie z.B. die Luft. Ist hingegen Ausschließbarkeit zu bejahen, während jedoch keine Rivalität gegeben ist, spricht man von sog. Klubgütern. Der Einzelne kann dabei selbst und allein über das Gut entscheiden, jedoch verbraucht er es nicht endgültig, sodass auch andere noch Zugriff darauf haben. Darunter fallen beispielsweise ein Automobilclub mit seinen einzelnen Mitgliedern, von denen jedoch der Einzelne durch seinen Zugriff auf das Gut dieses nicht vollständig verbraucht. Auch alle anderen Mitglieder können gleichzeitig die zur Verfügung gestellten Güter nutzen. Liegen im Gegensatz zu erstgenannter Variante sowohl Ausschließbarkeit als auch Rivalität vor, handelt es sich eindeutig um rein private Güter, wie z.B. das eigene Kraftfahrzeug und Kraftstoffe. Letztlich kann es sein, dass bei einem Gut zwar die Ausschließbarkeit zu verneinen, hingegen die Rivalität als gegeben zu betrachten ist. Sodann spricht man von sog. Allmendegütern. Dabei kann der Einzelne nicht allein über den Zugriff auf das Gut entscheiden. Zugleich besteht jedoch Rivalität, da das Gut der Gefahr ausgesetzt ist, dass es durch den Zugriff vieler verbraucht wird und somit nicht mehr zur Verfügung steht. Klassische Beispiele für Allmendegüter sind überfüllte Straßen und Fischbestände in einem freien Gewässer mit freiem Zugang, vgl. hierzu und zur Herleitung des Begriffs des Allmendeguts http://de.wikipedia.org/w/index.php?oldid=131610709. Es ist mithin möglich, jedes Gut einer der vorgenannten Kategorien zuzuordnen.

660 Vgl. unter *Kapitel 3, Teil 4, III.1.*.

Grundsätze auf die Datenverwendung des Arbeitgebers im Rahmen des Beschäftigungsverhältnisses zu übertragen, was an dieser Stelle nochmals zusammengefasst werden soll.

Da es sich bei den aus einem vernetzten und dem Arbeitnehmer überlassenen Fahrzeug anfallenden Daten sämtlich um personenbezogene bzw. zumindest personenbeziehbare Daten handelt, greift hier der soeben genannte Aspekt der Ausschließbarkeit. Obwohl mangels Zuordnung der Daten diese grundsätzlich uneingeschränkt verwendet werden dürfen, gilt gerade für personenbezogene Daten eine Ausnahme. Es bedarf insoweit für den Zugriff auf solche Daten entweder eines gesetzlichen Erlaubnistatbestandes oder aber einer vom Arbeitnehmer erteilten Einwilligung.

Als Erlaubnistatbestand für sämtliche Zugriffsbefugnisse des Arbeitgebers auf personenbezogene Daten des Arbeitnehmers kommt nach dem aktuellen Stand des Bundesdatenschutzgesetzes nur die Vorschrift des § 32 Abs. 1 Satz 1 BDSG[661] in Betracht. Die Neuregelungen der Vorschriften über den Beschäftigtendatenschutz in einem eigenen Gesetz entsprechend den §§ 32 bis 32l BDSG-E sind bislang nicht in Kraft getreten.

An dieser Stelle sollen lediglich die Zugriffsbefugnisse des Arbeitgebers auf Daten *„für Zwecke des Beschäftigungsverhältnisses“* im Sinne des § 32 Abs. 1 Satz 1 BDSG nochmals aufgegriffen werden. Insoweit kommt daneben eine Anwendung der Erlaubnistatbestände des § 28 BDSG nicht in Betracht.[662]

Damit ein Arbeitgeber Zugriff auf Daten für Zwecke des Beschäftigungsverhältnisses hat, muss eine solche Datenverwendung erforderlich sein. Wie bereits gezeigt[663], muss eine entsprechende Datenverwendung sich als mehr als nützlich aber weniger als zwingend notwendig erweisen. Insbesondere im Zusammenhang mit vernetzten Kraftfahrzeugen als Dienstfahrzeug des Arbeitnehmers wird die Ortung von Kraftfahrzeugen – aber auch von Mobiltelefonen – mittels GPS den klassischen Fall der Datenverwendung im Arbeitsverhältnis darstellen. Vor allem für Speditionen stellt dies einen immensen wirtschaftlichen Vorteil dar, wenn die einzelnen Arbeitnehmer mit ihren Fahrzeugen geortet werden können, um dadurch auch kurzfristige Routenänderungen vornehmen und so beispielweise die Lieferkette auf Zuruf optimieren zu können. Denkbar sind aber

661 Vgl. unter *Kapitel 3, Teil 3, I.1.c).*
662 Vgl. unter *Kapitel 3, Teil 3, I.1.c)(i).*
663 Vgl. unter *Kapitel 3, Teil 3, I.1.c)(iii).*

im vernetzten Fahrzeug auch unzählige andere Datenverwendungen. Diese müssen sich letztlich in jedem Einzelfall an den aufgestellten Grundsätzen messen lassen.

4. Folgeprobleme

Trotz der bereits getroffenen eindeutigen Feststellung, dass für Daten keine rechtliche oder faktische Zuordnung getroffen werden kann und für deren Verwendung nur bei vorhandenem Personenbezug bzw. vorhandener Personenbeziehbarkeit ein gesetzlicher Erlaubnistatbestand erfüllt sein oder eine Einwilligung vorliegen muss, stellt sich in diesem Zusammenhang darüber hinaus noch eine Vielzahl weitergehender Fragen.[664]

Es stellt sich die Frage, wer über die Zuordnung der Daten als personenbezogen bzw. personenbeziehbar entscheidet und ob es dafür auf eine Beurteilung der Daten durch den Betroffenen ankommt. Selbstredend würde die Beurteilung des Personenbezugs von Daten aus Sicht des Betroffenen oftmals differenzierter ausfallen, als dies bei der Beurteilung durch die verantwortliche Stelle der Fall wäre. Auch bezüglich der Feststellung von verantwortlicher Stelle und Betroffenem an sich ist zu problematisieren, wer diese Feststellung treffen soll und auf wessen Sicht es ankommen muss. Um dem Schutzgedanken des Datenschutzrechts gerecht zu werden, hat eine Beurteilung des Personenbezugs sowie der Feststellung, wer Betroffener und wer verantwortliche Stelle ist, aus Sicht des Betroffenen stattzufinden. Würde man dazu allein auf die Sicht der verantwortlichen Stelle abstellen, würde der Schutzgedanke des Datenschutzrechts unterlaufen. Es ist allein der Betroffenen, der hier die notwendige Kenntnis und Reichweite der Datenverwendung einschätzen muss. Eine anhand objektiver Kriterien vorzunehmende Feststellung ähnlich der Auslegung nach dem objektiven Empfängerhorizont würde dem nicht ausreichend Rechnung tragen.

Zudem ist beispielgebend die Frage zu stellen, ob für nicht personenbezogene Daten ein Verfallsdatum anzunehmen ist. Im Hinblick auf personenbezogenen Daten existiert eine explizite Regelung zur Löschung derselben in § 35 BDSG. Sofern Daten jedoch an sich zunächst keinen Personenbezug aufweisen, besteht trotz allem die Gefahr, dass diese zu einem späteren Zeitpunkt beispielsweise durch Anwendung von Big Data im vernetzten Fahrzeug einen Personenbezug oder zumindest eine Personenbeziehbarkeit aufweisen können. Dies gilt insbesondere für technische Daten, die zunächst keine Rückschlüsse

---

664 Die hier aufgeführten Folgeprobleme sollen im Rahmen der Untersuchung nicht weiter vertieft werden.

auf die Person des Fahrers ermöglichen.[665] Bringt man diese mit anderen Daten in Verbindung, kann daraus im Einzelfall möglicherweise der Fahrer identifiziert werden, sodass in diesem Fall der Personenbezug eindeutig vorliegt. Somit besteht auch für rein technische Daten das Risiko der Herstellung eines Personenbezugs zu einem späteren Zeitpunkt. Das Risiko erhöht sich, je mehr Daten gesammelt und je länger diese gespeichert werden. Insofern ist tatsächlich die Annahme eines Verfallsdatums für nicht personenbezogene Daten zu diskutieren. Dies erscheint im Hinblick auf den Schutzgedanken des Datenschutzrechts begrüßenswert. Auch Daten ohne Personenbezug dürfen nicht über Jahre hinweg genutzt werden ohne dass nach einer gewissen Zeit eine erneute Überprüfung bzw. Löschung derselben zu erfolgen hat. Ansonsten bestünde auf ungewisse Zeit für den etwaig Betroffenen die Gefahr, dass ohne sein Wissen plötzlich ein Personenbezug hergestellt werden kann. Dies kann nicht mit dem Sinn und Zweck des Datenschutzrechts in Einklang gebracht werden. Es ist mithin auch für Daten ohne Personenbezug ein Verfallsdatum zu generieren. Über den Zeitraum, nach dem solche Daten zu löschen sein sollten, könnte ebenfalls diskutiert werden. Es erscheint jedoch sinnvoll aufgrund der rasanten Entwicklung im technischen Bereich und im Zusammenhang mit vernetzte Fahrzeugen hier von einem eher kurzen Zeitraum auszugehen, nachdem auch Daten ohne Personenbezug zu löschen oder einer Überprüfung zu unterziehen sind und im Falle eines sodann etwaig festgestellten Personenbezugs an den Tatbeständen des Bundesdatenschutzgesetzes zu messen sein müssen.

Teil 5: Potenziell betroffene Daten im vernetzten Fahrzeug

Um im nächsten Schritt die Datenverwendung im Kraftfahrzeug zu untersuchen, soll an dieser Stelle zusammenfassend ein Überblick gegeben werden, welche Daten im vernetzten Fahrzeug potentiell betroffen sind.[666]

Hierbei können sämtliche Daten außer Acht gelassen werden, die in Bezug auf Fahrer oder Fahrzeug nur von geringem Interesse sind und gerade kein Konfliktpotenzial in sich bergen.[667] Für diese Daten können Betroffene keinen datenschutzrechtlichen Schutz beanspruchen, weil diese Daten ihrer Natur nach bereits nicht geeignet sind, als Eingriffe in das allgemeine Persönlichkeitsrecht des Betroffenen eingestuft zu werden.

---

665 Vgl. unter *Kapitel 2, Teil 5, I.*.

666 Vgl. dazu insgesamt unter *Kapitel 2.*

667 Vgl. unter *Kapitel 2, Teil 2, I.1.a)* sowie *Kapitel 2, Teil 2, I.2.a).*

Lediglich solche Daten, die eine gewisse Schwelle überschreiten und als Eingriff in vorbezeichnetes Recht zu werten sind, lösen die Überprüfung der Verwendung solcher Daten anhand der Vorschriften des Bundesdatenschutzgesetzes aus.

Letztere sind zunächst sämtliche Daten zum Fahrverhalten des Fahrzeugführers. Insbesondere sind hier generierte Daten zu Beschleunigung und Verzögerung relevant. Diese lassen sich ableiten aus den Daten, die beispielsweise durch den Gaspedalsensor oder den Bremsdrucksensor erzeugt werden. Aber auch anhand der Daten des Längs- und Querbeschleunigungs-Sensors im Rahmen des ESP lassen sich Rückschlüsse auf das Fahrverhalten des Fahrzeugführers schließen.

Aber auch Bewegungs- und Positionsdaten sind als potentiell betroffenen Daten einzuordnen. Diese spielen im Bereich der Car to Car-Technologie eine bedeutende Rolle. Durch sie wird es erst möglich, mit anderen Kraftfahrzeugen zu kommunizieren, indem die eigene Position festgestellt und teilweise an andere Kraftfahrzeuge in der Nähe übermittelt werden, um beispielsweise einen Stau, Unfall oder sonstige potenzielle Gefahrenquellen mitzuteilen. Lokale Verkehrsmeldungen können insoweit über WLAN weitergegeben werden mit der Folge, dass auch den anderen beteiligten Verkehrsteilnehmern die eigenen Positionsdaten zur Verfügung gestellt werden.

Durch die Verbindung des Kraftfahrzeugs mit Mobiltelefonen oder anderen sog. Smart Devices kommen als potentiell betroffene Daten auch die Mobilfunkdaten aus mit dem Kraftfahrzeug integrierten SIM[668] in Betracht. Dazu gehören insbesondere Kontaktdaten, die vom Mobiltelefon auf das Kraftfahrzeug übertragen werden und Kontaktdaten Dritter enthalten ebenso wie personenbezogene Daten des Nutzers für den Fall, dass über das Mobiltelefon und somit letztlich über das Kraftfahrzeug Daten aus Emails oder sozialen Netzwerken abgerufen werden.

In Bezug auf die geplante Technik, das Anlassen des Fahrzeugmotors von einem Atemalkoholtest abhängig zu machen, lassen sich dieser Kategorie sämtliche Login-Daten zuordnen. Auch diese sind insgesamt als potenziell betroffene Daten im vernetzten Fahrzeug zu sehen. Dies betrifft auch sämtliche Dienste, die ein Login vor der Nutzung erfordern. Sollte ein solcher Login durch Passwörter, Fingerabdrücke oder auch Retinascan Voraussetzung für die Nutzung sein, stellen die daraus zu generierenden Daten

668 Vom englischen *„subscriber identity module“* für Teilnehmer-Identitätsmodul“, vgl. https://de.wikipedia.org/wiki/SIM-Karte.

ebenfalls solche Daten dar, die für den Fahrzeugführer und Dritte relevant sind. Hierbei handelt es sich vorwiegend auch um die besonders geschützten medizinischen Daten des Fahrzeugführers.

Potenziell betroffen ist auch der Minimaldatensatz beim verpflichtenden Einbau des eCall-Systems in Kraftfahrzeuge.

All diese Daten bedürfen eines besonderen Schutzes über die Vorschriften des Bundesdatenschutzgesetzes.

Teil 6: Datenverwendung im Kraftfahrzeug

Die Datenverwendung im Kraftfahrzeug erfolgt auf verschiedene Art und Weise. Vorangestellt sei jedoch nochmals, dass den Fahrzeughaltern mangels Information seitens der Hersteller weitgehend unbekannt ist, welche Daten im Kraftfahrzeug von den Herstellern überhaupt erhoben, verarbeitet, ausgewertet und gespeichert werden mit der Folge, dass Halter erst in etwaigen Gewährleistungs- oder Haftungsprozessen mit den sodann als Beweismittel gegen sie gerichteten Daten konfrontiert werden.[669] Grundsätzlich kann jedoch unabhängig davon, ob und was tatsächlich an Daten gespeichert und verarbeitet wird, zwischen drei Formen der Datenverwendung im Kraftfahrzeug unterschieden werden.

I. Formen der Datenverwendung im Kraftfahrzeug

Ausgehend von dem Wissen des Betroffenen kann hinsichtlich einer Datenverwendung im Kraftfahrzeug differenziert werden zwischen der geheimen und ohne Wissen des Betroffenen vorgenommenen Datenverwendung sowie der offiziellen und mit Wissen des Betroffenen erfolgten Datenverwendung. Zuletzt kann auch eine freiwillige und mit Einwilligung des Betroffenen stattfindende Datenverwendung seitens des Herstellers vorliegen.

1. Geheime Datenverwendung

Soweit eine geheime Datenverwendung stattfindet, erfolgt dies ohne Einwilligung und zusätzlich auch ohne Wissen des Betroffenen. Bei den auf diesem Weg verwendeten Daten handelt es sich regelmäßig um Daten für Fahrzeugfunktionen, die sich regelmä-

669 Vgl. *Mielchen*, SVR 2014, S. 81–87 (82).

ßig mangels Herrschaft über die verwendeten technischen Systeme dem Zugriff des Betroffenen entziehen und über deren Verwendung der Betroffene nicht durch die verantwortliche Stelle im Rahmen der Datenschutzerklärung aufgeklärt wurde.[670] Zudem handelt es sich dabei um Daten, bezüglich derer dem Betroffenen in aller Regel das notwendige Fachwissen fehlt, um diese selbständig verwenden zu können.

Diese Daten können nur vom Hersteller und den Werkstätten ausgelesen werden. Dies betrifft insbesondere die in Steuergeräten von ABS, ESP und Airbag sowie Motorsteuergeräten generierten Daten.[671] Die Hersteller schützen diese Daten vehement vor externen Zugriffen, um selbständig eine optimale wechselseitige Anpassung der unterschiedlichen Einzelsysteme aufeinander gewährleisten zu können und entscheiden somit darüber, welche Daten als *„flüchtig“*, *„fest“* oder *„semifest“* einzustufen sind und damit über die Speicherdauer und Speicherlogik je nach Art und Schwere des Fehlers.[672] Die Automobilindustrie verweigerte bislang nach *Arentz* sogar der Polizei nach tödlichen Verkehrsunfällen den Zugang zu den Computerprogrammen, die eine Auswertung der Bordelektronik möglich machen würde.[673]

Solche Daten sind zwar zunächst technischer Natur und betreffen insoweit lediglich sachliche Verhältnisse und fahrzeugbezogene Informationen. Allerdings besteht auch bei reinen Messdaten die Gefahr, dass diese im Falle eines Unfalls oder durch sog. Big Data-Anwendungen mit anderen – ebenfalls an sich unverfänglichen – Daten verknüpft werden und dadurch ein Personenbezug zum Fahrer hergestellt und ein Profil von diesem erstellt werden kann. Dies insbesondere auch im Hinblick darauf, dass durch diese Messdaten aus Steuergeräten ein Rückschluss auf das Fahrverhalten des Betroffenen möglich wird. Sobald die Daten jedoch zu einer einzelnen Person zuordenbar sind, dürfen diese Daten nach dem Bundesdatenschutzgesetz nur noch in Ausnahmefällen verwendet werden.[674]

Betroffen von der geheimen Datenverwendung ist zunächst der Nutzer des Kraftfahrzeugs. Für den Fall, dass das Kraftfahrzeug jedoch von mehreren Personen genutzt

---

670 Vgl. *Kremer*, RDV 2014, S. 240–252 (248).
671 Vgl. unter *Kapitel 2, Teil 2, I.*.
672 Vgl. *Mielchen*, SVR 2014, S. 81–87 (82).
673 So Franz-Josef Arentz (KHK), in seinem Vortrag im Rahmen des GDP-Verkehrsforums am 19.12.2012, vgl. http://www.gdp.de/gdp/gdpnrw.nsf/id/DE_Experten-fordern-Zugang-der-Polizei-zu-digitalen-Unfallspuren-.
674 So Prof. Michael Brenner, vgl. http://www.auto.de/magazin/datenspeicherung-in-pkw-als-rechtliche-grauzone/.

wird, hat eine Zuordnung der personenbezogenen Daten zu erfolgen, um den jeweils Betroffenen zu benennen. Stellt sich heraus, dass die Daten dem falschen Nutzer zugeordnet wurden, hat gegebenenfalls eine Berichtung im Sinne des § 35 BDSG zu erfolgen.

Verantwortliche Stelle sind in diesen Fällen die Hersteller bzw. Werkstätten. Da es maßgeblich auf die sog. Datenhoheit ankommt[675], wäre es ebenfalls denkbar, dass die Datenhoheit dem Betroffenen bleibt und die Datenverwendung durch Hersteller und Werkstatt lediglich im Auftrag des Betroffenen erfolgt.

Eine Einwilligung in die geheime Datenverwendung wird in der Praxis nicht wirksam eingeholt werden können. Dazu fehlt es an einer freien und informierten Erklärung.[676] Wenn der Betroffenen nicht darüber aufgeklärt wird, dass überhaupt Daten generiert und verwendet werden, kann in Bezug darauf keine wirksame Einwilligung erteilt werden, da ein Hinweis auf den Zweck der diesbezüglichen Datenverwendung nicht erfolgen wird und auch nicht in notwendigem Umfang erklärt werden kann ohne darzustellen, welche Daten überhaupt verwendet werden.

2. Offizielle Datenverwendung mit Wissen des Betroffenen

Im Gegensatz zu der geheimen Datenverwendung erfolgt die offizielle Datenverwendung mit Wissen des Betroffenen. Dabei ist zwischen den Fällen zu unterscheiden, in denen der Betroffene im Rahmen einer Datenschutzerklärung seitens der verantwortlichen Stelle darüber aufgeklärt wurde und solchen, in denen eine Datenverwendung durch die verantwortliche Stelle offenkundig ist.

Von einer auf Seiten des Betroffenen vorliegenden Offenkundigkeit kann insbesondere bei Anwendungen und Diensten intelligenter Verkehrssysteme ausgegangen werden, die von dem Betroffenen selbst aktiv in Betrieb genommen werden und die die Verwendung der Daten kenntlich macht, wie dies z.B. bei Daten aus Servicefunktionen und bei Infotainment-Systemen der Fall ist, in denen der Betroffene sein Handy als sog. Smart Device mit dem Kraftfahrzeug verbindet und anschließend über das Kraftfahrzeug Nachrichten oder Emails versendet, telefoniert oder soziale Netzwerke nutzt.[677]

---

675 Vgl. unter *Kapitel 3, Teil 2, II.2.*.
676 Vgl. unter *Kapitel 3, Teil 3, II.1.b).*
677 Vgl. *Kremer*, RDV 2014, S. 240–252 (248).

Beispielhaft kann an dieser Stelle auch das sog. eCall-System vorgebracht werden. Im Rahmen des eCall-Systems wird der sog. Minimaldatensatz an die örtlich zuständige Notrufabfragestelle übertragen.[678] Dabei werden insbesondere Name und Positionsdaten des Betroffenen an die Leitstelle übermittelt. Es ist diesbezüglich keine Anonymität vorgesehen, jedoch ist aus Datenschutzgründen ein *„schlafendes System“* beabsichtigt, das sich nur im Falle eines Unfalls aktiv einschaltet und Daten überträgt.[679]

Betroffener ist in diesen Fällen der Fahrer des Kraftfahrzeugs. Sollten sich noch weitere Insassen im Fahrzeug befinden, wird dies gegebenenfalls anhand der Sensoren des Kraftfahrzeugs, wie z.B. dem Gurtschlosssensor oder dem Sitzbelegungssensor erkannt und diese Informationen ebenfalls an die Leitstelle übermittelt. Auch anhand der Übertragung der Positionsdaten kann für die weiteren Insassen ebenfalls von einer Betroffenheit im Sinne des Bundesdatenschutzgesetzes ausgegangen werden.

Im Anwendungsbereich des eCalls ist die Leitstelle als verantwortliche Stelle zu qualifizieren. Für den Fall der Speicherung der Daten in der Leitstelle könnte jedoch auch die Polizei die Daten aufgrund der bestehenden Gesetzeslage zur Aufklärung des Unfalls die Daten beschlagnahmen mit der Folge, dass in der Praxis damit eine gezwungene Datenweitergabe bei Unfällen hergestellt und nahezu automatisch durch das eigene Fahrzeug der Polizei belastendes Material zur Verfügung gestellt würde.[680]

Eine Einwilligung ist hier nicht einzuholen. Es handelt sich um ein gesetzlich vorgeschriebenes System, das gesetzlich legitimiert ist und somit die Erteilung einer Einwilligung entbehrlich macht. Im Falle einer im Sinne des § 4 Abs. 1 BDSG angeordneten Datenverwendung im Rahmen des eCalls hat der Einzelne keine Befugnis, sich dagegen zu wehren, indem er seine Einwilligung nicht erteilt. Allerdings gilt dies nur für tatsächliche Notfälle, die zum jetzigen Zeitpunkt alleiniger Zweck des eCall-Systems sind. Sollte darüber hinaus mit dem Minimaldatensatz eine anderweitige Verwendung gewollt sein, so ist dazu eine vertragliche Regelung bzw. die Erteilung einer Einwilligung des Betroffenen notwendig.

Es besteht hier auch die Möglichkeit, dass der Betroffenen von der verantwortlichen Stelle im Rahmen einer Datenschutzerklärung über die Datenverwendung aufgeklärt

678 Vgl. unter *Kapitel 2, Teil 5, III.*.
679 Vgl. *Mielchen*, SVR 2014, S. 81–87 (83).
680 Vgl. *Mielchen*, SVR 2014, S. 81–87 (84).

wird. Im Zusammenhang mit der Datenverwendung in vernetzten Kraftfahrzeugen haben sich der Verband der deutschen Automobilindustrie und die Datenschutzaufsichtsbehörden zur Verbesserung der Transparenz über Datenumgänge im Zusammenhang mit Kraftfahrzeugen auf eine Muster-Information über Datenspeicher im Fahrzeug geeinigt, die in Zukunft in die Betriebsanleitungen der neuen Fahrzeuge mit aufgenommen werden soll:

> *"Eine Vielzahl elektronischer Komponenten Ihres Fahrzeugs enthalten Datenspeicher, die technische Informationen über Fahrzeugzustand, Ereignisse und Fehler temporär oder dauerhaft speichern. Diese technischen Informationen dokumentieren im Allgemeinen den Zustand eines Bauteils, eines Moduls, eines Systems oder der Umgebung:*
>
> - *Betriebszustände von Systemkomponenten (z.B. Füllstände)*
> - *Statusmeldungen des Fahrzeugs und von dessen Einzelkomponenten (z.B. Radumdrehungszahl/ Geschwindigkeit, Bewegungsverzögerung, Querbeschleunigung)*
> - *Fehlfunktionen und Defekte in wichtigen Systemkomponenten (z.B. Licht und Bremsen,)*
> - *Reaktionen des Fahrzeugs in speziellen Fahrsituationen (z.B. Auslö- sen eines Airbags, Einsetzen der Stabilitätsregelungssysteme)*
> - *Umgebungszustände (z.B. Temperatur)*
>
> *Diese Daten sind ausschließlich technischer Natur und dienen der Erkennung und Behebung von Fehlern sowie der Optimierung von Fahrzeugfunktionen. Bewegungsprofile über gefahrene Strecken können aus diesen Daten nicht erstellt werden.*
>
> *Wenn Serviceleistungen in Anspruch genommen werden (z.B. bei Reparaturleistungen, Serviceprozessen, Garantiefällen, Qualitätssicherung), können diese technischen Informationen von Mitarbeitern des Servicenetzes (einschließlich Hersteller) aus den Ereignis- und Fehlerdatenspeichern mit speziellen Diagnosegeräten ausgelesen werden. Dort erhalten Sie bei Bedarf weitere Informationen. Nach einer Fehlerbehebung werden die Informationen im Fehlerspeicher gelöscht oder fortlaufend überschrieben.*
>
> *Bei der Nutzung des Fahrzeugs sind Situationen denkbar, in denen diese technischen Daten in Verbindung mit anderen Informationen (Unfallprotokoll, Schä-*

den am Fahrzeug, Zeugenaussagen etc.) - gegebenenfalls unter Hinzuziehung eines Sachverständigen - personenbeziehbar werden könnten.

Zusatzfunktionen, die mit dem Kunden vertraglich vereinbart werden (z.B. Fahrzeugortung im Notfall), erlauben die Übermittlung bestimmter Fahrzeugdaten aus dem Fahrzeug."[681]

Diese Muster-Information würde dem Betroffenen im Rahmen des Abschlusses des Kaufvertrages über ein neues Kraftfahrzeug mit der Betriebsanleitung überlassen. Der Betroffene wird hier über die Datenverwendung aufgeklärt. Allerdings ist es hier als problematisch anzusehen, ob die vorgelegte Muster-Information auch tatsächlich als ausreichend betrachtet werden kann.

Dies ist nach diesseitiger Auffassung nicht der Fall. Zunächst bezieht sich die Muster-Information lediglich auf rein technische Daten. Dass auch technische Daten teilweise ohne Hinzuziehung weiterer Informationen schon an sich fahrerbezogen sind und teilweise Konfliktpotenzial im datenschutzrechtlichen Sinne aufweisen, wurde bereits dargestellt.[682] Dies wird im Rahmen der Muster-Information nicht dargelegt. Der Betroffene gewinnt hier den Eindruck, es gebe im Kraftfahrzeug lediglich rein technische Daten, die nichts über ihn und seine Fahrweise aussagen.

Dem muss jedoch entgegengetreten werden. Durch die immer weiter voranschreitende technische Entwicklung ist durch die Anwendung von Big Data innerhalb der Steuergeräte eines Kraftfahrzeuges auch eine Profilbildung möglich. Entgegen der Erklärung in der Muster-Information ist dies bereits innerhalb des Kraftfahrzeugs möglich. Dazu ist es nicht notwendig, andere Informationen, wie z.B. Unfallprotokolle oder Zeugenaussagen hinzuzuziehen. Dies wird aber in der vorliegenden Muster-Information so dargestellt und könnte somit dem Betroffenen suggerieren, dass erst im Falle eines durch die Polizei aufgenommenen Unfalls eine Personenbeziehbarkeit hergestellt werden könne. Der Betroffenen wird nicht ausreichend darüber aufgeklärt, dass es auch bei unfallfreier Fahrt zur Verwendung von personenbezogenen Daten kommen kann.

Auch wird in der Muster-Information nicht auf die Vielzahl an Fahrerassistenzsystemen eingegangen, ohne die neue Kraftfahrzeuge heutzutage nicht mehr auskommen. Auch

---

681 Vgl. http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/Muster-Information_Fahrzeugdatenspeicher.pdf.

682 Vgl. unter *Kapitel 2, Teil 2, I.2.b).*

dabei kann bereits ein Personenbezug hergestellt werden. Dies lässt die Muster-Information völlig außen vor. Insoweit muss hier davon ausgegangen werden, dass eine solche Datenschutzerklärung aus datenschutzrechtlicher Sicht nicht ausreichend ist.

3. Datenverwendung mit Einwilligung des Betroffenen

Zuletzt ist auch eine Datenverwendung mit Einwilligung des Betroffenen möglich. Die erteilte Einwilligung muss in diesen Fällen den Anforderungen des § 4 Abs. 1 BDSG entsprechen und demnach freiwillig und mit Wissen des Betroffenen erfolgen. Entsprechende Einwilligungen werden in der Praxis bisher nahezu ausschließlich für Daten aus Service-Funktionen im Zusammenhang mit dem Kauf eines Kraftfahrzeugs eingeholt, wie z.B. im Zusammenhang mit der Datenverwendung bei den sog. Telematik-Tarifen, die im Vorhinein die Installation einer Telematik-Box im Kraftfahrzeug erfordern.[683] Obwohl der Versicherer in diesen Fällen lediglich abstrakte Scoringpunkte übermittelt bekommt, setzt dies zunächst jedoch die Erfassung, Speicherung und Auswertung der fahrzeug- und fahrerbezogenen Daten voraus.[684] Ebenfalls in diese Kategorie ist auch die Datenverwendung bei Service-Funktionen wie im Kraftfahrzeug eingebauter Dashcams oder dem sog. Alcolock[685] zu fassen.

In diesen Fällen werden unterschiedliche Daten verwendet. Im medizinischen Bereich ist in jeden Fall davon auszugehen, dass dort ein Personenbezug besteht und auch eine datenschutzrechtliche Betroffenheit des Autofahrers besteht. Es ist insoweit bei vorgenannten Service-Funktionen festzustellen, dass personenbezogene Daten verwendet werden. Diese stellen sich je nach Funktion unterschiedlich dar.

Betroffener im datenschutzrechtlichen Sinne ist bei Telematik-Tarifen der Versicherungsnehmer, der nicht identisch mit dem Fahrer sein muss. In allen anderen Fällen ist der Fahrer als Betroffener anzusehen. Sind weitere Insassen im Kraftfahrzeug anwesend, sind auch diese als Betroffene einzustufen, sofern sich die jeweilige Service-

683 Vgl. *Kremer*, RDV 2014, S. 240–252 (248).

684 Vgl. *Mielchen*, SVR 2014, S. 81–87 (83).

685 Vgl. bezüglich beider Service-Funktionen unter *Kapitel 2, Teil 2, I.2.b).* Hinsichtlich Dashcams ist nochmals festzustellen, dass der Einsatz solcher Kameras datenschutzrechtlich an § 6b Abs. 1 Nr. 3 und Abs. 3 BDSG zu messen ist und eine nicht ausschließlich für persönliche oder familiäre Tätigkeiten vorgenommene Aufnahme unzulässig ist, da in diesen Fällen die schutzwürdigen Interessen der Verkehrsteilnehmer gegenüber den Interessen des Autofahrers an einer Weitergabe des Filmmaterials zur Dokumentation eines Unfallhergangs überwiegen, vgl. http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/26022014_UnzulaessigkeitDashcams.pdf;jsessionid=D34611C5895F788BE08BF833F6F7621B.1_cid354?__blob=publicationFile&v=1.

Funktion auch auf sie erstreckt. Dies setzt allerdings voraus, dass auch die übrigen Insassen wirksam in die jeweilige Datenverwendung eingewilligt haben.

Als verantwortliche Stelle ist im Zusammenhang mit Telematik-Tarifen der Versicherer einzuordnen. Dieser hat alleinigen Zugriff auf die mit Einwilligung des Betroffenen erlangten Daten und stellt diese dem Betroffenen lediglich auf einem Webportal zur Überprüfung bereit.[686]

Bei den sog. Alcolocks könnten sowohl der Fahrer als auch der Halter als verantwortliche Stelle in Betracht kommen. Würde man auf den Fahrer abstellen, wäre dieser zugleich als Betroffener wie auch als verantwortliche Stelle einzustufen. Dies hätte zur Folge, dass der Schutz des Bundesdatenschutzgesetzes nicht greifen würde. Es besteht gerade kein Schutzbedürfnis für den Fall, dass der Betroffene für seine eigene Datenverwendung verantwortlich ist. Dies kann für die durch den Einsatz sog. Alcolocks geplante Datenverwendung nicht Sinn und Zweck sein.

Insoweit muss unterstellt werden, dass diese Service-Funktion derart ausgestaltet ist, dass ein selbsttätiges An- und Abschalten durch den Fahrer nicht möglich ist und der Start des Kraftfahrzeugs davon abhängt, dass der Atemalkoholtest durchgeführt und sozusagen bestanden wird. Es handelt sich bei den im Kraftfahrzeug eingebauten Geräten um sog. medizinische Sensoren, welche höchstpersönliche Daten generieren. Diese umfänglich aus dem Anwendungsbereich des Datenschutzrechts herauszunehmen würde dazu führen, dass der Fahrer allein für den Schutz dieser Daten verantwortlich wäre. Dies kann von ihm nicht erwartet werden.

Noch dazu liegt hier die Entscheidungsbefugnis hinsichtlich der Datenverwendung auch tatsächlich beim Halter. Er entscheidet im Zweifel darüber, ob sein Kraftfahrzeug mit diesem Service-System ausgestattet wird und erteilt diesbezüglich seine Einwilligung. Zweck und Mittel der Datenverwendung werden dadurch durch ihn festgelegt. Dass es für die Benutzung auf den Fahrer ankommt, spielt insoweit keine Rolle. Der Fahrer hat keine Handhabe, selbst darüber zu entscheiden, ob er von dieser Service-Funktion Gebrauch machen will. Zwar werden seine Daten verarbeitet, was ihn zum Betroffenen macht. Allerdings kann nicht von einer Entscheidungsbefugnis über die Datenverwendung auf seiner Seite ausgegangen werden.

686 Vgl. *Mielchen*, SVR 2014, S. 81–87 (84).

Im Zusammenhang mit den sog. Dashcams wird darauf abzustellen sein, ob es eine Möglichkeit für den Fahrer gibt, die Kamera selbsttätig ein- bzw. auszuschalten. Für diesen Fall könnte die Entscheidungsbefugnis über die Datenverwendung dem Fahrer zugeordnet werden. Lediglich für den Fall, dass der Fahrer keinen Einfluss darauf hat, liegt die Entscheidungsbefugnis hier beim Halter.

Eine Einwilligung liegt in diesem Fall vor und wird erteilt von Halter, Fahrer oder Versicherungsnehmer. Sollte die Einwilligung nicht wirksam erteilt worden sein, besteht keine Erlaubnis zur Datenverwendung.

Als problematisch erweist sich in diesem Fall die Tatsache, dass ein Kraftfahrzeug durchaus von weiteren verschiedenen Personen genutzt werden kann. Um hier von einer wirksamen Einwilligungserteilung ausgehen zu können, müssten auch diese Nutzer in die Datenverwendung eingewilligt haben. Dies stellt sich im Hinblick auf spätere Nutzer und auch noch zu entwickelnde Anwendungen schwierig dar. Möglich wäre hier eine Textanzeige beim Start des Kraftfahrzeugs, die über die Datenverwendung hinsichtlich einzelner Service-Funktionen aufklärt und die der Fahrer sodann per Knopfdruck bestätigen und damit seine Einwilligung in die Datenverwendung erklären kann. Es müsste jedoch dabei ein Zusammenhang zwischen Lesen und Losfahren sichergestellt werden. Ob insoweit noch von einer freiwilligen Erklärung des Fahrers ausgegangen werden kann, darf sicherlich bezweifelt werden. Dem Fahrer geht es darum, das Fahrzeug starten und bedienen zu können. Wenn es dafür zwingend erforderlich wäre, eine Einwilligung in die Datenverwendung in Bezug auf verschiedene Service-Funktionen zu erteilen, schränkt ihn dies in erheblichem Maße in seiner allgemeinen Handlungsfreiheit ein.

Unabhängig davon ist es jedoch auch fraglich, ob über eine Textanzeige, die bei jedem Start erscheint und eine Bestätigung des Fahrers erfordert, das Ziel einer umfassenden Aufklärung erreicht werden kann. Dies erscheint nicht praktikabel. Denkbar wäre daneben die Lösung durch Einsatz einer PIN. Diese könnte dem Käufer bzw. Halter bei Vertragsschluss überlassen werden. Gleichzeitig erfolgt in diesem Zusammenhang eine wirksame Aufklärung mit sich daran anschließender Erteilung der Einwilligung seitens des Käufers. Aber auch diese Herangehensweise löst die Problematik späterer Nutzer nicht. Die Verpflichtung zur Erteilung einer wirksamen Einwilligung kann zwar weitergegeben werden. Wem gegenüber ein Dritter jedoch in diesen Fällen seine Einwilligung

erteilen muss, ist ebenfalls nicht klar. Dabei muss wieder darauf abgestellt werden, wer die Herrschaft über die Datenverwendung besitzt. Würde man diese dem Hersteller zusprechen, ergäbe sich daraus wiederum die Problematik, dass der Hersteller keine Möglichkeit hätte, zu kontrollieren, ob tatsächlich in jedem Einzelfall von einem Dritten wirksam eine Einwilligung erteilt wurde. Es besteht mithin im Hinblick auf diese Problematik weiterer Klärungsbedarf.

Zuletzt stellt sich auch an dieser Stelle die Problematik der wirksamen Erteilung einer Einwilligung durch Beschäftigte[687]. Die Freiwilligkeit einer solchen Einwilligung muss bezweifelt werden, wenn der Beschäftigte ohne Erteilung seiner Einwilligung nicht arbeitsfähig wäre und es sich somit um eine arbeitsrechtliche Einstellungsvoraussetzung handelt. Deshalb sollte für diese Fälle der Weg über eine Betriebsvereinbarung gegangen werden. Darin könnten die Modalitäten einer Datenverwendung im Zusammenhang mit Dienstfahrzeugen geregelt werden. Allerdings darf dadurch nicht die individuelle Einwilligung umgangen werden. Als geschäftliche Grundlage kann jedoch eine solche Datenverwendung nur im Rahmen einer Betriebsvereinbarung geregelt werden, wenn an anderer Stelle auf eine Datenverwendung verzichtet wird.

II. Politische Sichtweise

Auch in der Politik ist die Datenverwendung in Bezug auf Daten aus vernetzten Kraftfahrzeugen brisantes Thema. Allerdings wurde die Frage, *„wie verhindert werden kann, dass Bewegungsprofile oder Halterinformationen der Fahrzeuge ungehindert gespeichert oder verarbeitet werden“* von der Bundesregierung bislang *„noch nicht vertieft geprüft“*.[688] Es werden jedoch bereits beispielsweise im Rahmen der *„Digitalen Agenda“*[689] im Zusammenhang mit den sog. Intelligenten Verkehrssystemen Vorschläge für Handlungsmaßnahmen zur Einführung des Automatisierten Fahrens am Runden Tisch *„Automatisiertes Fahren“* abgestimmt.[690]

Zum Thema automatisiertes Fahren startete das Bundesministerium für Verkehr und digitale Infrastruktur zusammen mit der Automobilindustrie und der Digitalwirtschaft das *„Digitale Testfeld Autobahn“* auf der A9 in Bayern – ein Autobahnabschnitt als

687 Vgl. unter *Kapitel 3, Teil 3, II.3.*.
688 BT-Drs. 18/706 vom 05.03.2014, S. 11, http://dip21.bundestag.de/dip21/btd/18/007/1800706.pdf.
689 Vgl. http://www.bmwi.de/DE/Themen/Digitale-Welt/digitale-agenda.html..
690 Vgl. Bundesministerium für Verkehr und digitale Infrastruktur: Fortschrittsbericht: Digitale Agenda für Deutschland vom 24.03.2015.

erste intelligente und volldigitalisierte Straße, die über modernste Sensorik, Mobilfunkübertragung der neueste Generation und alle Technologien für das automatisierte und vernetzte Fahren verfügt.[691]

Zudem wurde im September 2015 seitens der Bundesregierung die *„Strategie automatisiertes und vernetztes Fahren“* vorgelegt.[692] Darin werden neben den Zielen[693] auf dem Weg zum automatisierten und vernetzten Fahren auch Handlungsfelder und Maßnahmen aufgezeigt, die zur Umsetzung erarbeitet werden müssen. Neben der Verbesserung der digitalen Infrastruktur hin zu einem Breitbandausbau und einer bis zum Jahr 2018 flächendeckend sichergestellten Grundversorgung mit mindestens 50Mbit/s sieht die Bundesregierung hier in Bezug auf den internationalen sowie nationalen Rechtsrahmen Handlungsbedarf insbesondere in der Erweiterung des Begriffs des Fahrers gemäß Art. 1 lit. v WÜ-StV und in der Erhöhung der zulässigen Höchstgeschwindigkeit für den Einsatz automatisierter Fahrsysteme von bislang 10 km/h auf 130 km/h sowie der Ermöglichung des automatisierten Spurwechsels, wobei die Anpassung der UN/ECE-Regeln und dort insbesondere der Regelungen zur Lenkung (UN/ECE-Regel 79) bereits initiiert sei und weiter verfolgt werde.[694]

Ein Antrag der Fraktionen der CDU/CSU und SPD vom 26.01.2016 *(„Intelligente Mobilität fördern – Die Chancen der Digitalisierung für den Verkehrssektor nutzen“)* deutet jedoch darauf hin, dass sich die Bundesregierung in der Zwischenzeit tatsächlich vertiefter mit der Thematik des Datenschutzes bei vernetzten Fahrzeugen auseinandergesetzt hat. Zum Aspekt *„Datenschutz und Datensicherheit“* heißt es in dem Antrag:

> *„Personenbezogene Daten, die vom Fahrzeug erzeugt werden, sollten nur mit Zustimmung des Betroffenen und bestehend auf einer gesetzlichen Grundlage pseudonymisiert erhoben werden dürfen, so dass u. a. die Erstellung von Bewegungsprofilen mit einem direkten Personenbezug nicht möglich ist.“*[695]

---

691 Vgl. https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/automatisiertes-fahren.pdf?__blob=publicationFile.

692 Vgl. https://www.bmvi.de/SharedDocs/DE/Publikationen/StB/broschuere-strategie-automatisiertes-vernetztes-fahren.pdf?__blob=publicationFile.

693 *„Leitanbieter bleiben, Leitmarkt werden, Regelbetrieb einleiten“*, vgl. https://www.bmvi.de/SharedDocs/DE/Publikationen/StB/broschuere-strategie-automatisiertes-vernetztes-fahren.pdf?__blob=publicationFile.

694 Vgl. https://www.bmvi.de/SharedDocs/DE/Publikationen/StB/broschuere-strategie-automatisiertes-vernetztes-fahren.pdf?__blob=publicationFile, S. 14 und S. 16.

695 Vgl. BT-Drs. 18/7362, http://dip21.bundestag.de/dip21/btd/18/073/1807362.pdf.

Die Formulierung *„nur mit Zustimmung des Betroffenen und bestehend auf einer gesetzlichen Grundlage“* könnte hier bei strenger Wortlautauslegung darauf hindeuten, dass die Bundesregierung die Lösung der Problematik in einer Verschärfung des nationalen Datenschutzes sieht. Denn nach dem derzeit geltenden Bundesdatenschutzgesetz nach § 4 Abs. 1 BDSG stehen beide Alternativen als Erlaubnistatbestände alternativ nebeneinander. Der Betroffene kann in die Datenverarbeitung einwilligen oder diese ist gesetzlich erlaubt. Insoweit könnte auch davon ausgegangen werden, dass die Bundesregierung hier ebenfalls von einer alternativen Geltung entsprechend den geltenden Regelungen ausgeht und insgesamt die in dem Antrag verwendete Formulierung einen redaktionellen Fehler darstellt.

Sollte dies nicht der Fall sein[696] und die Bundesregierung tatsächlich eine Verschärfung der datenschutzrechtlichen Bestimmungen in Betracht ziehen, ist davon auszugehen, dass eine solche Verschärfung gegen EU-Recht und dort Art. 7 DS-RL verstoßen würde. Nach Art. 7 DS-RL darf die Verarbeitung personenbezogener Daten lediglich erfolgen, wenn eine der dort genannten Voraussetzungen erfüllt ist. Hierzu entschied der Europäische Gerichtshof schon mit Urteil vom 24.11.2011, dass die Mitgliedstaaten weder neue Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten neben Art. 7 DS-RL einführen, noch zusätzliche Bedingungen stellen dürfen, die die Tragweite eines der sechs in diesem Artikel vorgesehenen Grundsätze verändern würden.[697] Hier müsste allerdings davon ausgegangen werden, dass eine verpflichtend kumulative Erfüllung der Erlaubnistatbestände der Einwilligung und der gesetzlich vorgesehenen Erlaubnis nicht mit Art. 7 DS-RL vereinbar wäre. Es würde sich vielmehr um eine zusätzliche und demnach nach der vorgenannten Rechtsprechung des Europäischen Gerichtshofs unzulässige Bedingung handeln. Denn nach Art. 7 ist die Zulässigkeit der Datenverarbeitung von „*einer*“ der dort genannten Voraussetzungen abhängig. Würden nunmehr allerdings auf nationaler Ebene mehrere kumulative Voraussetzungen gefordert, geht dies über die europarechtlichen Regelungen hinaus. Insoweit ist hier bei der Auslegung der Anfrage zugunsten der nationalen Regelungen davon auszugehen, dass es sich lediglich um ein redaktionelles Versehen handelt und die Bun-

696 Auch in der Beschlussempfehlung und Bericht des Ausschusses für Verkehr und digitale Infrastruktur (15. Ausschuss) hierzu erfolgte keine Klarstellung diesbezüglich, vgl. BT-Drs. 18/7635 vom 23.02.2016, http://dip21.bundestag.de/dip21/btd/18/076/1807635.pdf.

697 Europäischer Gerichtshof, Urteil vom 24.11.2011, Aktenzeichen C-468/10 und C-469/10, EuZW 2012, S. 37-40.

desregierung hier keine grundlegende Verschärfung des Datenschutzes im vorgenannten Sinne plant.

III. Ethische Sichtweise

Auch aus ethischer Sichtweise müssen die Vernetzung von Kraftfahrzeugen untereinander und mit Intelligenten Verkehrssystemen und die sich daraus ermöglichende Datenverwendung kritisch betrachtet werden. Es droht der *„Gläserne Autofahrer"*. Durch die Anwendung von Big Data ist eine Verschiebung von Macht weg vom Individuum hin zu de facto unkontrollierbaren und intransparenten Strukturen zu befürchten, die es so noch nicht gegeben hat.[698] Aber auch der Aspekt, dass von den daran verdienenden Verantwortlichen suggeriert wird, dass der Verlust der Privatsphäre eine unweigerliche Folge des Einsatzes von Computer und Netzen sei[699], ist kritisch zu hinterfragen. Bei den Betroffenen wird oftmals der Eindruck erweckt, die technische Weiterentwicklung sei *„normal"* und diene in jedem Fall dem Betroffenen selbst und seiner Sicherheit bzw. seinen Interessen. Dass sich ein Einzelner dagegen wehren könnte und auch ohne weiteres auf bestimmte Datenverwendungsvorgänge aus seinem Kraftfahrzeug verzichten könnte, ist diesem aufgrund der bisher nicht geschaffenen Transparenz nicht möglich. Letztlich muss die Vernetzung von Fahrzeugen und Infrastruktur aus ethischer Sicht kritisch hinterfragt werden. Es muss dabei ein Gleichgewicht geschaffen werden, zwischen der tatsächlich notwendigen Technik und zusätzlichen Diensten und Systemen, auf die der Betroffenen getrost verzichten könnte, wenn ihm dies denn bewusst gemacht würde. Die bereits jetzt bestehenden erheblichen ethischen Bedenken in diesem Zusammenhang werden zunächst bestehen bleiben.

IV. Datenverwendung in der Praxis

Wirft man dabei einen Blick auf die Datenverwendung in der Praxis, so lässt sich feststellen, dass unbenommen des Standpunktes der Bundesregierung die Daten tatsächlich ohne weiteres verwendet werden. Viele Automobilhersteller verarbeiten die Daten ihrer Service-Angebote selbst in eigenen abgeschlossenen Serversystemen. Dies hat zur Folge, dass viele Fahrer überhaupt nicht wissen, welche Daten überhaupt erhoben oder gespeichert werden. Die Modalitäten halten die Hersteller geheim. Zu nennen sind hier die

698 So *Rieger*, APuZ 15-16/2013, S. 3-7 (7).
699 So *Rieger*, APuZ 15-16/2013, S. 3-7 (4).

Angebote *„Audi connect“* von Audi[700], *„FleetBoard“* von Daimler[701] und *„DynaFleet“* von Volvo[702].

Aber auch im Bereich der Telematik-Anwendungen werden Daten verwendet. Im Zusammenhang mit dem Telematik-Tarif *„S-Drive-Service“* der Sparkassen DirektVersicherung[703] sammeln die Versicherer eine Menge Daten. Dem Versicherer liegen dabei die Kundendaten[704] vor. Der Telematik-Anbieter als beauftragter externer Dienstleister hat faktisch Zugriff auf Fahrzeug- und Fahrtdaten[705] sowie zusätzlich auf die Kunden-ID. Die Übermittlung der Daten in Form der von ihm errechneten Score-Werte an den Versicherer erfolgt aufgrund der Erlaubnistatbestände der §§ 28, 29 BDSG. Dabei wird monatlich der errechnete Score-Wert inklusive Kilometerstand und verbunden mit der Kunden-ID an den Versicherer übertragen.[706]

Insoweit lässt sich feststellen, dass die Datenverwendung in der Praxis stattfindet. Obwohl aus politischer Sicht noch keine explizite Einstufung vorgenommen oder ein Standpunkt festgelegt wurde, werden in der Praxis die aus dem vernetzten Fahrzeug bereits jetzt anfallenden Daten auf verschiedene Art und Weise verwendet.

V. Daten in der Strafverfolgung

Zuletzt sollte auch ein Blick auf das Schicksal der Daten im Rahmen der Strafverfolgung geworfen werden. Je mehr Daten Aufschluss über Verhalten, Aufenthalt und über das sonstige Profil eines Autofahrers geben, desto höher ist selbstredend auch das Interesse der Strafverfolgungsbehörden an solchen Daten.

Die Schwierigkeit besteht im vorliegenden Zusammenhang jedoch darin, dass die Daten nicht wie bei der gewöhnlichen Durchsuchung in Papierform vorliegen, sondern von den Strafverfolgungsbehörden erst *„sichtbar“* gemacht bzw. auf internen oder externen

---

700 Vgl. http://www.audi.de/de/brand/de/neuwagen/layer/audi-connect-lp.html.

701 Vgl. http://www.fleetboard.de/.

702 Vgl. http://www.volvotrucks.com/trucks/germany-market/de-de/Online_services/dynafleet/Pages/Default.aspx.

703 Vgl. unter *Kapitel 2, Teil 5, II.*.

704 Darunter fallen u.a. die Kunden-ID, der Name und die Anschrift des Kunden, dessen Handynummer für den Notfall, die E-Mail-Adresse sowie weitere Versicherungsvertragsdaten.

705 Dies betrifft die Position des Fahrzeugs, Uhrzeit, Geschwindigkeit bzw. Geschwindigkeitsüberschreitungen, Brems- und Beschleunigungsverhalten, zurückgelegte Kilometer und die Fahrtrichtung.

706 Vgl. dazu insgesamt http://www.welt.de/finanzen/versicherungen/article121912643/Die-erste-vom-Fahrverhalten-abhaengige-Versicherung.html.

Speichermedien gesucht werden müssen, die sich wiederum auch an einem anderen Speicherort im In- oder Ausland befinden können.[707]

Zunächst ist festzustellen, dass Daten ebenso wie körperliche Gegenstände sichergestellt und beschlagnahmt werden können. Grundsätzlich beziehen sich Sicherstellung und Beschlagnahme von Beweisgegenständen nach § 94 StPO auf Gegenstände und damit auf bewegliche Sachen jeder Art.[708] Die Sicherstellung bzw. Beschlagnahme kann sich dabei nach der Rechtsprechung des Bundesverfassungsgerichts aber auch auf Datenträger und Computerausdrucke beziehen. Dazu entschied das Bundesverfassungsgericht:

> *„§ 94 StPO erlaubt auch die Sicherstellung von Daten auf behördeneigenen Datenträgern. Der Wortsinn gestattet es, als „Gegenstand" des Zugriffs auch nichtkörperliche Gegenstände zu verstehen. Der Wortlaut wird durch die Annahme, auch unkörperliche Gegenstände seien von § 94 StPO erfasst, schon im Hinblick auf die Unterscheidung gegenüber dem engeren Begriff der (körperlichen) Sache nicht überschritten."*[709]

Dies ist insoweit als höchstrichterlich geklärt anzusehen.

Es stellt sich jedoch die Frage, bei wem die Daten sichergestellt oder beschlagnahmt werden können. Dafür ist es relevant, wo die Informationen in Form der Daten liegen. Eine Sicherstellung bzw. Beschlagnahme kommt nur beim Gewahrsamsinhaber in Betracht. Im Zusammenhang mit der Datenverwendung in vernetzten Kraftfahrzeugen kommen hier insbesondere Hersteller, Werkstätten, Halter und Fahrer des Kraftfahrzeugs in Betracht. Unter Gewahrsam im strafrechtlichen Sinne versteht man die vom Herrschaftswillen getragene tatsächliche Sachherrschaft.[710] Sachherrschaft kann aber auch in diesem Zusammenhang nur angenommen werden, wenn eine Zugriffsmöglichkeit und eine Entscheidungsbefugnis für die Daten besteht.[711] Insoweit ist der Gewahrsamsinhaber, bei dem Daten sichergestellt oder beschlagnahmt werden können, nach diesen Kriterien zu ermitteln.

---

707 Vgl. *Bär*, ZIS 2011, S. 53–59 (53).

708 Vgl. *Meyer-Goßner/Schmitt*: Strafprozessordnung, [58]2015, § 94, Rn. 4.

709 Bundesverfassungsgericht, Beschluss vom 12.04.2005, Aktenzeichen 2 BvR 1027/02., NJW 2005, S. 1917-1923 (1920) und Bundesverfassungsgericht, Beschluss vom 18.02.2003, Aktenzeichen 2 BvR 372/01, NStZ-RR 2003, S. 176-177 (177).

710 Vgl. *Fischer*: Strafgesetzbuch, [61]2014, § 242, Rn. 11.

711 Vgl. unter *Kapitel 3, Teil 2, II.2.*.

Soweit die Frage geklärt werden kann, bei wem eine Beschlagnahme zu erfolgen hat, schließt sich daran die Problematik an, in welchem Umfang und unter welchen Voraussetzungen eine Beschlagnahme möglich ist.

Es sollen an dieser Stelle die Grenzen der Sicherstellung bzw. Beschlagnahme, die sich aus allgemeinen strafprozessualen Grundsätzen ergeben, aufgezeigt werden. Dabei spielt insbesondere der sog. *„nemo tenetur“*[712]-Grundsatz eine Rolle. Der Sicherstellung bzw. Beschlagnahme kann hier der Grundsatz entgegenstehen, dass sich niemand selbst einer Straftat bezichtigen muss. Dies gilt für den Beschuldigten einer Straftat ebenso wie nach der Vorschrift des § 55 Abs. 1 StPO für den Zeugen, der im Rahmen seines Auskunftsverweigerungsrechts bei einer Aussage weder sich selbst noch einen Angehörigen, der nicht Beschuldigter ist, belasten muss.[713]

Der Fahrer könnte im Rahmen der Aufklärung eines Verkehrsunfalls von seinem eigenen Kraftfahrzeug überführt werden, wenn er beispielsweise vorträgt, der Unfallgegner habe ihm die Vorfahrt genommen, es sich aber durch Auslesen der Daten herausstellt, dass der Fahrer selbst zu schnell gefahren ist. In diesem Fall würde ihn letztlich auch die zivilrechtliche Haftung treffen. Ohne das Auslesen der Daten hätte eventuell gar nicht der Beweis geführt werden können, dass der Fahrer selbst die zulässige Höchstgeschwindigkeit weit überschritten hat und somit auch in zivilrechtlicher Hinsicht nicht haftbar wäre bzw. ihm in strafrechtlicher Hinsicht keine Schuld nachgewiesen werden könnte.

Allerdings ist zu beachten, dass es in diesen Fällen wohl gar nicht im Ermessen des Fahrers selbst stehen würde, ob die Daten preisgegeben werden. Denn dazu wäre es erforderlich, dass der Fahrer selbst auch eine Zugriffsmöglichkeit auf die Daten hat. Da aber bereits[714] festgestellt wurde, dass solch technische Daten, wie die Geschwindigkeitsmessung, nur dem Hersteller zur Verfügung stehen und in nahezu allen Fällen der Betroffenen überhaupt keine Kenntnis von einer etwaigen Speicherung hat, führt dies dazu, dass dem Betroffenen letztlich keine Entscheidungsbefugnis darüber zukommt, ob solche Daten für die Beweisführung genutzt werden oder nicht. Insoweit wäre hier an eine gerichtliche Anordnung zur Mitwirkung des Herstellers gemäß § 142 ZPO denkbar

---

712 *„Nemo tenetur se ipsum accusare“*, § 136 Abs. 1 Satz 2, § 163a Abs. 4 Satz 2 und § 243 Abs. 5 Satz 1 StPO.

713 Vgl. *Meyer-Goßner/Schmitt*: Strafprozessordnung, [58]2015, § 55, Rn. 1.

714 Vgl. unter *Kapitel 3, Teil 6, I.1.*.

mit der Folge, dass der Hersteller die Geräte auslesen und anhand der Geschwindigkeitsdaten zu einem gegen den betroffenen Fahrer sprechenden Ergebnis kommt und dieser dadurch durch sein eigenes Kraftfahrzeug verraten würde, ohne vorher darüber in Kenntnis gesetzt worden zu sein, dass eine solche Möglichkeit und Gefahr für ihn besteht.[715]

Ähnlich stellt sich die Problematik im Hinblick auf den nemo tenetur-Grundsatz auch im Zusammenhang mit Telematik-Tarifen der Versicherungen dar. Dort weiß der Betroffenen zwar von der Datenverwendung, gerade auch, weil er diese ausdrücklich gewünscht hat und sich dadurch günstigere Versicherungsbedingungen erhofft. Allerdings ist auch hier mit einer Weitergabe der Daten seitens der Versicherung zu rechnen, die bereits zum jetzigen Zeitpunkt bereitwillig den Strafverfolgungsbehörden Auskunft über Angaben machen, die ein Geschädigter im Rahmen seiner Schadensanzeige ihnen gegenüber getätigt hat.[716]

All dies beeinträchtigt das den Betroffenen schützende Grundrecht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG. Der Betroffene soll dem Grunde nach selbst darüber entscheiden können, welche Daten von ihm preisgegeben werden oder welche er der Verwendung durch andere vorenthalten will. Dieses Grundrecht wird jedoch massiv beeinträchtigt, wenn die Strafverfolgungsbehörden über Umwege an die Daten des Betroffenen herankommen und diese gegen ihn einsetzen können. Dieses Vorgehen beeinträchtigt noch dazu den nemo tenetur-Grundsatz und ein bestehendes Aussageverweigerungsrecht.

Es ist somit dringend erforderlich, diesem Vorgehen Grenzen zu setzen. Grenzen bestehen jedoch bereits in Form der durch die Vorschriften der §§ 94 ff. StPO aufgestellten Voraussetzungen einer wirksamen und ordnungsgemäßen Sicherstellung bzw. Beschlagnahme. Herausragende Bedeutung hat in diesem Zusammenhang der zu wahrende Grundsatz der Verhältnismäßigkeit. Es wird verlangt, dass die Maßnahme zur Erreichung des angestrebten Ziels geeignet und erforderlich sein muss und dass der mit ihr verbundene Eingriff nicht außer Verhältnis zur Bedeutung der Sache und zur Stärke des Tatverdachts stehen darf.[717] Zudem muss die Maßnahme notwendig sein, d.h. es muss

---

715 So *Mielchen*, SVR 2014, S. 81–87 (85).

716 Vgl. *Mielchen*, SVR 2014, S. 81–87 (85).

717 Bundesverfassungsgericht, Beschluss vom 03.09.1991, Aktenzeichen 2 BvR 279/90, NStZ 1992, S. 91-92 (92).

abgewogen werden, ob der im Raum stehende Verdacht so gewichtig und die in Rede stehende Straftat so gefährlich ist, dass öffentliche Interessen an der vollständigen Aufklärung einer Tat so erheblich sind, dass dahinter eine Beschränkung von Grundrechten hingenommen werden muss.[718] Jedoch ist es ebenso erforderlich, dass ein Anfangsverdacht einer Straftat vorliegt, der auf einer Tatsachengrundlage beruht, aus der sich die Möglichkeit der Tatbegehung durch den Beschuldigten ergibt, sodass eine bloße Vermutung nicht ausreicht.[719] Allerdings erscheint diese notwendige Voraussetzung im Zusammenhang mit einer Datenverwendung aus vernetzten Kraftfahrzeugen nicht hinreichend zum Schutz des Betroffenen. Denn die Daten werden zukünftig u.a. durch das eCall-System und die Telematik-Tarife leicht zugänglich sein und zudem besteht bei jedem Verkehrsunfall ein gewisser Anfangsverdacht dafür, dass ein Fahrer den Unfall verschuldet haben muss, sodass zu befürchten ist, dass zukünftig ein Datenabruf durch Sicherstellung bzw. Beschlagnahme routinemäßig und flächendeckend bei jedem Unfall durchgeführt wird.[720]

Insoweit ist hier dringender Handlungsbedarf gegeben, um der schrankenlosen und leichtfertigen Datenverwendung Einhalt zu gewähren und diese nicht ohne weitere Prüfung durch das Vorliegen der Voraussetzungen der Sicherstellung bzw. Beschlagnahme zu rechtfertigen. Ein Zugriff auf die Daten erfolge laut *Weichert* zwar derzeit nur in Einzelfällen, dies werde jedoch zunehmen.[721] Zu beachten ist auch, dass diese Kompetenzen nur den staatlichen Strafverfolgungsbehörden zur Verfügung stehen. Die vorgenannten Grundsätze können nicht auf ein Handeln Privater übertragen werden, da die weitreichenden Eingriffsmöglichkeiten der Strafverfolgungsbehörden dem Vorbehalt der richterlichen Genehmigung unterliegen.[722] Insoweit können sich im vorliegenden Zusammenhang Arbeitgeber nicht der Informationen bedienen, die ihnen beispielsweise durch Anbieter von Telematik-Tarifen zur Verfügung gestellt werden.

Es lassen sich außerdem auch weitere Szenarien bilden. Sollten Anbieter von Telematik-Tarifen anhand der von ihnen erstellten Auswertungen Prognosen erstellen können, aus denen sich ergibt, dass ein bestimmter Fahrer aller Wahrscheinlichkeit nach in ab-

---

718 Bundesverfassungsgericht, Teilurteil vom 05.08.1966, Aktenzeichen 1 BvR 586/62, 610/63, 512/64, NJW 1966, S. 1603-1616 (1613).

719 Bundesverfassungsgericht, Beschluss vom 23.01.2004, Aktenzeichen 2 BvR 766/03, NStZ-RR 2004, S. 143-144 (143).

720 Vgl. *Mielchen*, SVR 2014, S. 81–87 (86).

721 Vgl. *Eicher*, ADAC Motorwelt, (4/2014), S. 16–20 (18).

722 Vgl. *Weißgerber*, NZA 2003, S. 1005–1009 (1007).

sehbarer Zeit einen Unfall verursachen wird, stellen sich die Fragen, wie mit einer solchen Prognose umzugehen sein würde und ob insoweit Möglichkeiten bestünden, dem zuvorzukommen.

Hinsichtlich einer etwaigen Alkoholsucht eines Kraftfahrzeugfahrers kann die Fahrerlaubnisbehörde auf Grundlage der Vorschrift des § 13 FeV die Durchführung einer medizinisch-psychologischen Untersuchung (MPU) fordern. Dafür ist es bereits ausreichend, wenn die Gesamtumstände Zweifel daran erkennen lassen, dass der Betroffenen das Führen von Fahrzeugen und einen die Fahrsicherheit beeinträchtigenden Alkoholkonsum nicht hinreichend sicher trennen kann.[723] Dies könnte für die Strafverfolgungsbehörden das Einstiegstor dafür sein, auch auf einen Hinweis der Anbieter von Telematik-Tarifen tätig zu werden, wenn nach deren Prognose mit einer Unfallverursachung des Betroffenen zu rechnen ist. Denkbar wäre ein solches Szenario allemal.

Im Hinblick auf die Behandlung von Daten in der Strafverfolgung sei zuletzt verwiesen auf den *„Leitfaden zum Datenzugriff“*[724] der Generalstaatsanwaltschaft München. Dieser Leitfaden bezog sich insbesondere auf den Datenzugriff für den Bereich der Telekommunikation. Darin wurde ohne jegliche Begründung Folgendes festgestellt:

> *„seit 12/2009 ist BMW selbst Netzprovider; ist die FIN (Fahrzeugidentifikationsnummer) bekannt, erfolgt eine Bestandsdatenabfrage bei BMW nach § 113 TKG; mittels dieser Daten kann eine TKÜ[725] Maßnahme nach § 100a StPO veranlasst werden.“*[726]

Diese Feststellungen betrafen die Ermittlungsmaßnahme der Kfz-Ortung für den Fall, wobei vorausgesetzt wurde, dass in dem Kraftfahrzeug ein SIM-Modul eingebaut ist, welches die Ortung ermöglicht. Dabei wird im Rahmen des Leitfadens u.a. auf die Systeme *„BMW-Assist“* / *„ConnectedDrive“* hingewiesen. Aufgrund der Tatsache, dass für dieses Vorgehen keine Begründung geliefert wurde, wurde dieser Aspekt aus dem Leitfaden entfernt.

---

723 Oberverwaltungsgericht Lüneburg, Beschluss vom 29.01.2007, Aktenzeichen 12 ME 416/06, DAR 2007, S. 227-228; vgl. auch *Dauer* in Hentschel: Straßenverkehrsrecht, [43]2015, § 13 FeV, Rn. 20.

724 Stand Juni 2011, vgl. https://www.vorratsdatenspeicherung.de/images/leitfaden_datenzugriff_voll.pdf.

725 TKÜ ist die Abkürzung für die sog. Telekommunikationsüberwachung.

726 Vgl. S. 7 des Leitfadens, https://www.vorratsdatenspeicherung.de/images/leitfaden_datenzugriff_voll.pdf.

Das behördliche Interesse an Daten aus dem vernetzten Fahrzeug ist bereits jetzt sehr groß und wird sich mit zunehmenden Möglichkeiten, im Rahmen vernetzter Fahrzeuge neue und vor allem eine Vielzahl mehr an Daten zu gewinnen, noch in erheblichem Maße steigern. So forderten bereits auf dem 52. Verkehrsgerichtstag (VGT) in Goslar Vertreter der Exekutive einen gesetzlich institutionalisierten Zugang zu verschiedenen Fahrzeugdaten um unter anderem Unfallhergänge besser rekonstruieren zu können.[727] Zu beachten ist hier, dass dies nur *„unter anderem"* der Unfallrekonstruktion dienen soll. Es ist ebenso denkbar, den Zugang zu den Daten aus vernetzten Fahrzeugen dazu zu nutzen, beispielsweise Geschwindigkeitsverstöße nachweisen zu können. Sollte ein solcher Zugang gemäß der Forderung der Vertreter auf dem 52. VGT gesetzlich geregelt und erlaubt werden, würde dies mit zunehmenden aufgrund der voranschreitenden Technik einhergehenden qualitativen sowie quantitativen Möglichkeiten dazu führen, dass auch vermehrt Anfragen auf Auskunft bzw. Überlassung von Daten bei Flottenbetreibern, Unternehmen sowie z.B. Mietwagenanbietern erwartet werden.

Zuletzt sei darauf hingewiesen, dass auf europäischer Ebene im Rahmen der Datenschutzreform auch eine neue Richtlinie[728] für Polizei und Justiz erlassen werden soll. Diese regelt die Verwendung personenbezogener Daten zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten. Auch daraus werden sich für die Zugriffe der Polizei und Justiz auf personenbezogene Daten neue Befugnisse und Grenzen ergeben.

Teil 7: Beteiligung von Arbeitnehmervertretungen bei Arbeitnehmerüberwachung durch technische Einrichtungen im Kraftfahrzeug

Für den praktischen Einsatz von vernetzten Fahrzeugen im Arbeitsverhältnis ist auch die Beteiligung von Arbeitnehmervertretungen zu beachten, sofern es durch den Einsatz technischer Einrichtungen im Kraftfahrzeug zur Überwachung der Arbeitnehmer kommt bzw. kommen kann. Dies und die sich fortentwickelnde technische Vernetzung im Bereich der Automobilindustrie sowie die Entwicklung neuer Technologien erfordern eine Anpassung des Umfangs der Mitbestimmung des Betriebsrates. Das zentrale Mittel zur

727 Vgl. http://www.car-it.com/daten-machen-autos-zu-zeugen-der-anklage/id-0039111.

728 *Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr vom 25.01.2012*,KOM (2012) 10 endg., http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:DE:PDF.

Umsetzung und Ausübung des Mitbestimmungsrechts des Betriebsrates ist wegen der unmittelbaren und zwingenden Geltung derselben nach § 77 Abs. 4 BetrVG die Betriebsvereinbarung.[729]

Es sollen an dieser Stelle verschiedene Fälle der Beteiligung von Arbeitnehmervertretungen[730] im Zusammenhang mit diversen praktischen Anwendungsfällen der vernetzten Automobiltechnik angesprochen werden. Relevant werden dabei die Vorschriften der §§ 94, 87 BetrVG sowie §§ 75, 76 BPersVG.

Damit verknüpft sollen nicht abschließend einige praktisch relevante Fallszenarien[731] dargestellt und anhand der zuvor vorgenommenen rechtlichen Erwägungen bewertet werden. Es ist danach zu fragen, welche Einsatzmöglichkeiten für vernetzte Fahrzeuge denkbar sind und wo insoweit Interessen seitens Hersteller, Arbeitgeber, Halter, Fahrer usw. bestehen.

I. Einwilligung in die Verwendung von personenbezogenen Daten im Personalfragebogen

Zunächst kann ein Mitbestimmungsrecht für die Verwendung von personenbezogenen Daten durch Erhebung eines Personalfragebogens relevant werden.

Nach § 94 BetrVG bedürfen Personalfragebogen[732] der Zustimmung des Betriebsrats. Der Begriff des Personalfragebogens ist weit auszulegen. Deshalb sind insoweit auch sämtliche formalisierten und standardisierten Informationserhebungen in Bezug auf Arbeitnehmerdaten unter die Vorschrift des § 94 BetrVG zu subsumieren.[733] Es ist dabei unerheblich, ob die standardisierten Fragen vom Arbeitgeber oder einem von ihm

729 Vgl. *Kania* in Müller-Glöge/Preis/Schmidt: Erfurter Kommentar zum Arbeitsrecht, [15]2015, § 87 BetrVG, Rn. 3.

730 In § 32 Abs. 3 BDSG erfolgt dahingehend ein ausdrücklicher Verweis auf die Beteiligung von Interessenvertretungen der Beschäftigten. Darunter fallen insbesondere der Betriebsrat (BetrVG), der Sprecherausschuss der leitenden Angestellten (SprAuG), der Personalrat (BPersVG/LPersVG) sowie Mitarbeitervertretungen im kirchlichen Bereich, vgl. *Kramer* in Weth: Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2014, S. 128 (Fn. 15).

731 Die Darstellung ist als nicht abschließend zu betrachten.

732 Als Personalfragebogen wird die formularmäßige Zusammenfassung von Fragen über die persönlichen Verhältnisse, insbesondere Eignung, Kenntnisse und Fähigkeiten einer Person bezeichnet, wobei solche Fragebogen nicht vom Tatbestand umfasst sind, die ausschließlich der Erhebung arbeitsplatz- oder betriebsbezogener Daten dienen, vgl. *Raab* in GK-BetrVG: Betriebsverfassungsgesetz, [10]2014, Band II, § 94, Rn. 16.

733 Vgl. *Klebe* in DKKW: BetrVG, [14]2014, § 93, Rn. 3.

beauftragten Dritten gestellt werden und in letztgenanntem Fall eventuell dem Arbeitgeber lediglich in anonymisierter Form zur Verfügung gestellt werden.[734]

Dies ist insbesondere für die sog. Telematik-Anwendungen, bei denen der Versicherer an den Arbeitgeber lediglich die aus den Daten des Kraftfahrzeugs ermittelten Daten anonymisiert und als Score-Wert weitergibt, relevant. Auch diese sind mithin vom Tatbestand des § 94 BetrVG erfasst. Die Zustimmung des Betriebsrates ist dabei einzuholen für jede Einführung und Änderung eines Personalfragebogens.[735]

Zu beachten ist auch das Verhältnis zu den Bestimmungen des Bundesdatenschutzgesetzes. Die Beteiligungsrechte der Interessenvertretungen der Beteiligten bleiben von den Regelungen des Bundesdatenschutzgesetzes unberührt.[736] Die Zustimmung des Betriebsrats wird also nicht deshalb entbehrlich, weil die Datenerhebung eventuell datenschutzrechtlich zulässig ist.[737] Unabhängig davon muss trotzdem die Zustimmung des Betriebsrats eingeholt werden.

Auch im Bundespersonalvertretungsgesetz existiert mit § 75 Abs. 3 Nr. 8 BPersVG eine entsprechende Regelung für ein Mitbestimmungsrecht.[738] Für die Mitbestimmung des Personalrates gilt hinsichtlich des Tatbestandes und des Inhalts der Mitbestimmung das zu § 94 BetrVG Gesagte entsprechend.[739]

Ein Mitbestimmungsrecht soll allerdings nach der Rechtsprechung des Verfassungsgerichtshofs Kassel zu verneinen sein, wenn die Erhebung auf die Weise geschieht, dass

---

734 Vgl. *Raab* in GK-BetrVG: Betriebsverfassungsgesetz, [10]2014, Band II, § 94, Rn. 16.; *Klebe* in DKKW: BetrVG, [14]2014, § 94, Rn. 3; Arbeitsgericht Bonn, Beschluss vom 31.10.2003, Aktenzeichen 2 BVGa 15/03, in: RDV 2004, S. 190-191 (190).

735 Vgl. *Kreuder* in Düwell: Betriebsverfassungsgesetz, [4]2014, § 94, Rn. 5.

736 Vgl. § 32 Abs. 3 BDSG.

737 Vgl. *Raab* in GK-BetrVG: Betriebsverfassungsgesetz, [10]2014, Band II, § 93, Rn. 19.

738 Danach hat der Personalrat mitzubestimmen über den Inhalt von Personalfragebogen für Arbeitnehmer, soweit keine gesetzliche oder betriebliche Regelung besteht. Der eingeschränkten Mitbestimmung unterliegt die Mitbestimmung des Personalrats über den Inhalt von Personalfragebogen für Beamte nach § 76 Abs. 2 Nr. 2 BPersVG. Die Einigungsstelle kann insoweit nach § 69 Abs. 4 Satz 3 und Satz 4 BPersVG nur zu einer Empfehlung mit anschließendem Letztentscheidungsrecht der obersten Dienstbehörde kommen, während im Rahmen des § 75 BPersVG ein uneingeschränktes Mitbestimmungsrecht besteht und die Einigungsstelle die abschließende Entscheidungsbefugnis hat, vgl. *Baden* in Altvater: BPersVG, [8]2013, § 76, Rn. 1. Es ist insoweit zu differenzieren zwischen dem Inhalt von Personalfragebogen für Arbeitnehmer und dem Inhalt derselben für Beamte, deren unterschiedliches Mitbestimmungsniveau jedoch nichts daran ändert, dass für beide Angelegenheiten ein einheitliches Mitbestimmungsverfahren durchgeführt und eine mögliche Differenzierung lediglich auf der letzten personalvertretungsrechtlichen Entscheidungsebene vorgenommen werden soll, so Bundesverwaltungsgericht, Beschluss vom 16.04.2008, Aktenzeichen 6 P 8.07, in: PersV 2008, S. 342-345 (345).

739 Vgl. *Baden* in Altvater: BPersVG, [8]2013, § 76, Rn. 85.

die Dienststelle selbst aus den ihr zur Verfügung stehenden Unterlagen die erforderlichen Daten zusammenstellt.[740]

Dem muss im vorliegenden Zusammenhang jedoch entgegengetreten werden. Insbesondere die mittlerweile technisch ohne weiteres mögliche Zusammenstellung einzelner Daten und die Erzeugung neuer Daten durch Anwendung von Big Data zeigt, dass auch in der Verknüpfung einzelner Daten ein eigenständiger Akt zu sehen ist. Dieser ist hier auch unter den vorliegenden Tatbestand zu subsumieren. Es kommt insoweit nicht auf das Vorliegen eines Personalfragebogens im ursprünglichen Sinne an. Vielmehr ist im Zusammenhang mit der Verwendung von Daten aus vernetzten Fahrzeugen durch Anwendung von Big Data darauf abzustellen, ob die Daten durch ein Verhalten des Arbeitnehmers generiert werden, welches sodann gleichzusetzen ist mit der Preisgabe von Daten im Rahmen eines Personalfragebogens.

Dies ist hier in jedem Fall gegeben, sofern sich anhand der Daten ein Rückschluss auf die Person des Fahrers oder deren Verhalten ergeben kann. Durch die Zusammenstellung einzelner Daten aus bereits vorhandenen Unterlagen können sich ungewollt neue Erkenntnisse bzw. Muster bilden, die dann wiederum auch das Persönlichkeitsrecht des Einzelnen beeinträchtigen können. Obgleich der betroffene Arbeitnehmer hier nicht selbständig und direkt die Daten zur Verfügung stellt, sondern die Daten aus technischen Systemverknüpfungen gewonnen werden, muss angenommen werden, dass auch die Zusammenstellung bereits vorhandener Daten dazu führt, dass Rückschlüsse gleich welcher Art gezogen werden können. Rückschlüsse lassen sich anhand des Verhaltens des Fahrers ziehen, was wiederum ein aktives Tun des Betroffenen erfordert. Dies ist letztlich gleichzusetzen mit der Beantwortung von Fragen in einem *„klassischen“* Personalfragebogen.

II. Einführung technischer Einrichtungen

Im Zusammenhang mit vernetzten Fahrzeugen wird jedoch schwerpunktmäßig die Frage der Mitbestimmung des Betriebsrates bei der Einführung und Anwendung techni-

740 Verfassungsgerichtshof Kassel, Beschluss vom 14.11.1990, Aktenzeichen BPV TK 974/90, CR 1991, S. 745-747 (746).

scher Einrichtungen relevant. Dies richtet sich nach der Vorschrift des § 87 Abs. 1 Nr. 6 BetrVG, der dem Betriebsrat ein Mitbestimmungsrecht[741] zuweist für die

> *„Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen".*

Ob ein Mitbestimmungsrecht besteht, richtet sich maßgeblich nach dem Zweck der Regelung. Zunächst ist festzustellen, dass die Vorschrift nicht vor jeder Überwachung schlechthin schützen soll, sondern dem Schutz vor den besonderen Gefahren der technischen Datenerhebung und Datenverarbeitung, soweit diese mit der Überwachung von Verhalten und Leistung der Arbeitnehmer unter Einsatz technischer Einrichtungen für das Persönlichkeitsrecht des Arbeitnehmers und für sein Recht auf freie Entfaltung der Persönlichkeit verbunden sind, dienen soll.[742] Der Schutz vor den Gefahren der modernen Datenverarbeitung schlechthin ist nicht Inhalt des Mitbestimmungsrechtes nach § 87 Abs. 1 Nr. 6 BetrVG.[743] Nach dem Sinn und Zweck der Vorschrift hat der Betriebsrat danach im Sinne eines präventiven Schutzes sowohl rechtlich unzulässige Eingriffe in das Persönlichkeitsrecht der Arbeitnehmer zu verhindern als auch zulässige Eingriffe auf das durch die betriebliche Notwendigkeit unabdingbar gebotene Maß zu beschränken.[744]

Bei der Zustimmung des Betriebsrates handelt es sich um eine Wirksamkeitsvoraussetzung für alle mitbestimmungspflichtigen Maßnahmen.[745] Deshalb können mitbestimmungswidrige Maßnahmen nicht nachträglich genehmigt werden und es besteht hinsichtlich mitbestimmungswidrig vom Arbeitgeber erlangter Informationen ein Beweisverwertungsverbot.[746] Sofern also ein Mitbestimmungsrecht des Betriebsrats angenommen wird, muss die Zustimmung des Betriebsrats zu mitbestimmungspflichtigen Maßnahmen vor der Durchführung derselben eingeholt werden. Ansonsten kann ein Arbeitnehmer sich erfolgreich gegen die Maßnahme zur Wehr setzen.

---

741 Vorliegend handelt es sich um ein erzwingbares Mitbestimmungsrecht, bei dem der Betriebsrat selbst die Initiative ergreifen und den Arbeitgeber zur Berücksichtigung des Mitbestimmungsrechts und der Durchführung einer dem Mitbestimmungsrecht unterliegenden Maßnahme auffordern kann, vgl. *Kramer* in Weth: Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2014, S. 171.

742 Bundesarbeitsgericht, Beschluss vom 11.03.1986, Aktenzeichen 1 ABR 12/84, NZA 1986, S. 526-530 (529).

743 Bundesarbeitsgericht, Beschluss vom 14.09.1984, Aktenzeichen 1 ABR 23/82, NJW 1985, S. 450-453 (451).

744 Vgl. *Fitting*: Betriebsverfassungsgesetz, [27]2014, § 87, Rn. 216.

745 Bundesarbeitsgericht, Beschluss vom 22.12.1980, Aktenzeichen 1 ABR 2/79, NJW 1981, S. 937-942 (942).

746 Vgl. *Klebe* in DKKW: BetrVG, [14]2014, § 87, Rn. 6.

1. Gesetzlicher Ausschluss des Mitbestimmungsrechts

Ein Mitbestimmungsrecht ist allerdings ausgeschlossen, wenn und soweit für die relevante Maßnahme eine gesetzliche oder tarifliche Grundlage besteht.

Dies betrifft vor allem ein etwaig bestehendes Mitbestimmungsrecht des Betriebsrats in Bezug auf den gesetzlich vorgeschriebenen und verpflichtenden Einbau des eCall-Systems.[747]

Da insoweit eine gesetzliche Regelung besteht, nach welcher der Einbau des eCall-Systems in alle neuen Kraftfahrzeuge und leichte Nutzfahrzeuge ab dem 31.03.2018 verpflichtend vorgeschrieben sein wird, besteht im Hinblick auf die Entscheidung, ob ein solches System vom Arbeitgeber eingebaut wird bzw. dieser den Einbau veranlasst, kein Mitbestimmungsrecht. Der Ausschluss des Mitbestimmungsrechts reicht jedoch nur soweit auch tatsächlich eine gesetzliche Regelung besteht. Darüber hinaus ist jeweils zusätzlich zu prüfen, ob ein Mitbestimmungsrecht des Betriebsrats eingreift.

a) Praktischer Anwendungsfall: eCall-System

Das eCall-System[748] ist aufgrund des gesetzlich vorgesehenen verpflichtenden Einbaus von praktisch hoher Relevanz. Im Hinblick auf eine großflächige Einführung des eCall-Systems wies die Europäische Kommission bereits darauf hin, dass die Einführung in diesen Fällen *„deutlich weniger“* als 100 Euro pro Neuwagen kosten werde.[749]

b) Szenarien

Die Einführung des verpflichtenden Einbaus eines eCall-Systems soll insbesondere der Reduzierung von Verkehrstoten und der Erhöhung der Verkehrssicherheit dienen.

Für den Nutzen und die Anwendbarkeit des eCall-Systems lassen sich daraus verschiedenste praktische Szenarien bilden. Zu denken ist dabei vor allem an Szenarien, in denen ein Fahrer mit seinem Kraftfahrzeug in der Nacht von der Straße abkommen und einen Unfall verursachen würde. Bei der befahrenen Strecke könnte es sich um eine Straße in einer abgelegenen Gegend handeln oder aber der Fahrer sein Kraftfahrzeug ungewollt einen Hang hinablenken, der nicht einsehbar sein könnte. Eine Aussicht auf

747 Vgl. unter *Kapitel 2, Teil 5, III.*.
748 Vgl. unter *Kapitel 2, Teil 5, III.*.
749 Vgl. http://www.spiegel.de/auto/aktuell/eu-legt-standards-fuer-automatischen-notruf-ecall-fest-a-905552.html.

Rettung besteht in diesen Fällen – insbesondere in der Nacht – nicht. Die Chance, dass potenzielle Retter den Unfall überhaupt bemerken, ist in solchen Fällen als sehr gering einzuschätzen. Ohne einen automatischen Notruf wäre der Fahrer hier darauf angewiesen, sich selbst zu helfen, was ihm unter Umständen aufgrund schwerer bzw. lebensgefährlicher Verletzungen nicht möglich sein würde. Einzig eine vorhandene manuell auszulösende Notruffunktion könnte dem Fahrer hier helfen, Rettungskräfte zu alarmieren. Da ein solcher jedoch von Seiten der Hersteller nur auf freiwilliger Basis einzubauen ist, wäre eine Rettung des Fahrers hier im Zweifel von dem von ihm gewählten Kraftfahrzeugmodell und dessen Ausstattung abhängig. Allerdings würde ein solches System insbesondere im Fall der Ohnmacht des Fahrers versagen.

Daran knüpft der Zweck der Einführung des eCall-Systems an. Bei dem eCall-System als automatischem Notruf ist ein Unfallopfer nicht auf sein eigenmächtiges Handeln oder andere Zufälligkeiten angewiesen. Das System informiert in diesen Fällen selbständig die nächstgelegenen Leitstelle und sendet den sog. MSD dorthin.[750] Die Leitstelle verfügt sodann ohne ein notwendiges Zutun des Unfallopfers über die erforderlichen Informationen, wie Position und Bewegungsrichtung des Kraftfahrzeugs, Art des Antriebs und die FIN. Diese Daten werden mindestens übertragen. Zusätzlich könnten in diesem Zusammenhang auch noch Daten zur Sitzbelegung und über die durch Sensoren ermittelten Verzögerungswerte zur Einschätzung des Schadensbildes übermittelt werden.

Ein weiteres mögliches Szenario in Bezug auf das eCall-System könnte darin zu sehen sein, dass im Zuge der technischen Weiterentwicklung eine Verbindung des eCall-Systems mit anderen Funktionen des Kraftfahrzeugs hergestellt werden könnte. Denkbar wäre eine Verknüpfung mit den im Kraftfahrzeug zukünftig vorhandenen medizinischen Sensoren[751]. Dadurch[752] könnte auch ohne den Eintritt eines Unfalls im verkehrsrechtlichen Sinne durch das System erkannt werden, wenn bei dem Fahrer ein medizinischer Notfall vorliegt und es könnte auch in diesen Fällen ein Notruf abgesetzt werden. Auf weite Sicht könnte in Verknüpfung mit der Funktion des autonomen Fahrens[753] sogar ein selbständiges Anhalten am Straßenrand im Falle eines medizinischen Notfalls als Möglichkeit in Betracht gezogen werden. Allerdings wäre es ebenfalls denkbar, dass

---

750 Vgl. unter *Kapitel 2, Teil 5, III.*.
751 Vgl. unter *Kapitel 2, Teil 2, I.2.b).*
752 Denkbar wäre hier eine Überwachung der Herzfunktion des Fahrers.
753 Vgl. unter *Kapitel 2, Teil 6*.

das Kraftfahrzeug durch Verwendung der Gesundheitsdaten bereits selbst die Feststellung treffen kann, ob noch ein Notarztwagen oder bereits ein Leichenwagen zu rufen ist, insbesondere weil im Todesfall der Rettungsdienst eventuell bereits bei einem weiteren schweren Unfall behilflich sein könnte.[754]

c) Rechtliche Würdigung

Die Europäische Union hat im Zusammenhang mit der Umsetzung des eCall-Systems eine Verordnung zur Einführung des eCall-Systems in Kraftfahrzeugen erlassen.[755] Dort heißt es in Art. 6 (Privatsphäre und Datenschutz):

> *„(1) Die Richtlinien 95/46/EG und 2002/58/EG bleiben von dieser Verordnung unberührt. Die Verarbeitung personenbezogener Daten durch das auf dem 112-Notruf basierende bordeigene eCall-System muss in jedem Fall den in diesen Richtlinien festgelegten Datenschutzvorschriften entsprechen.*
>
> *(2) Die nach dieser Verordnung verarbeiteten personenbezogenen Daten dürfen nur für die Handhabung der in Artikel 5 Absatz 2 Unterabsatz 1 genannten Notfallsituationen verwendet werden.*
>
> *(3) Die nach dieser Verordnung verarbeiteten personenbezogenen Daten dürfen nicht länger gespeichert werden, als dies für die Handhabung der in Artikel 5 Absatz 2 Unterabsatz 1 genannten Notfallsituationen erforderlich ist. Diese Daten werden vollständig gelöscht, sobald sie für diesen Zweck nicht mehr erforderlich sind.*
>
> *(4) Die Hersteller tragen dafür Sorge, dass das auf dem 112-Notruf basierende bordeigene eCall-System nicht rückverfolgbar ist und dass keine dauerhafte Verfolgung erfolgt.*
>
> *(5) Die Hersteller stellen sicher, dass im internen Speicher des auf dem 112-Notruf basierenden bordeigenen eCall-Systems die Daten automatisch und kontinuierlich gelöscht werden. Lediglich die drei letzten Positionen des Fahrzeugs dürfen gespeichert werden, soweit es für die Bestimmung der momentanen Position und der Fahrtrichtung zum Zeitpunkt des Vorfalls unerlässlich ist.*
>
> *(6) Bevor der eCall ausgelöst wird, dürfen diese Daten außerhalb des auf dem 112-Notruf basierenden bordeigenen eCall-Systems für keine Einrichtung zugänglich sein.*

---

754 So *Schwartmann/Ohr*: Datenschutzrechtliche Perspektiven des Einsatzes intelligenter Fahrzeuge, in: RDV 2015, S. 59–68 (65).

755 *Verordnung (EU) 2015/758 des Europäischen Parlaments und des Rates vom 29. April 2015 über Anforderungen für die Typgenehmigung zur Einführung des auf dem 112-Notruf basierenden bordeigenen eCall-Systems in Fahrzeugen und zur Änderung der Richtlinie 2007/46/EG*, ABl. L 123/84 vom 19.05.2015, http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32015R0758&from=DE.

(7) In das auf dem 112-Notruf basierende bordeigene eCall-System sind sowohl Technologien zur Stärkung des Datenschutzes einzubetten, um eCall-Anwendern den geeigneten Schutz zu bieten, als auch die erforderlichen Sicherungssysteme zur Verhinderung von Überwachung und Missbrauch.

(8) Der vom auf dem 112-Notruf basierenden bordeigenen eCall-System übermittelte MSD enthält ausschließlich die Mindestinformationen gemäß der Norm EN 15722:2011 „Intelligente Transportsysteme — Elektronische Sicherheit — Minimaler Datensatz (MSD) für den elektronischen Notruf eCall". Vom auf dem 112-Notruf basierenden bordeigenen eCall-System werden keine weiteren Daten übermittelt. Dieser MSD wird so gespeichert, dass er vollständig und dauerhaft gelöscht werden kann.

(9) Die Hersteller geben in der Betriebsanleitung klare und umfassende Informationen über die Verarbeitung von Daten durch das auf dem 112-Notruf basierende bordeigene eCall-System. Diese Informationen umfassen:

a) die Angabe der Rechtsgrundlage für die Datenverarbeitung;

b) die Angabe, dass das auf dem 112-Notruf basierende bordeigene eCall-System standardmäßig automatisch aktiviert wird;

c) die Ausgestaltung der vom auf dem 112-Notruf basierenden bordeigenen e-Call-System durchgeführten Datenverarbeitung;

d) den spezifische Zweck der eCall-Verarbeitung, der auf die in Artikel 5 Absatz 2 Unterabsatz 1 genannten Notfallsituationen beschränkt ist;

e) die Art der erhobenen und verarbeiteten Daten sowie die Empfänger derselben;

f) die Dauer der Speicherung der Daten im auf dem 112-Notruf basierenden bordeigenen eCall-System;

g) die Angabe, dass keine dauerhafte Verfolgung des Fahrzeugs erfolgt;

h) die Ausgestaltung der Wahrnehmung der Rechte der durch die Datenverarbeitung betroffenen Personen sowie die Kontaktstelle, die für die Bearbeitung von Zugangsanträgen zuständig ist;

i) jegliche sonstigen zusätzlichen Informationen hinsichtlich der Verfolgbarkeit, Verfolgung und Verarbeitung personenbezogener Daten im Zusammenhang mit der Bereitstellung eines TPS-eCalls und/oder anderer Dienste mit Zusatznutzen, für die der Eigentümer seine ausdrückliche Einwilligung erteilen muss und die im Einklang mit der Richtlinie 95/46/EG stehen müssen. Insbesondere ist zu berücksichtigen, dass es Unterschiede bei der Datenverarbeitung über das auf dem 112-Notruf basierende bordeigene eCall-System und über die bordeigenen TPS-eCall-Systeme oder andere Dienste mit Zusatznutzen geben kann.

(10) Damit es nicht zu Unklarheiten in Bezug auf die Zwecke und den Zusatznutzen der Verarbeitung kommt, werden vor der Inbetriebnahme des Systems die in Absatz 9 genannten Informationen für das auf dem 112-Notruf basierende bordeigene eCall-System und die bordeigenen TPS-eCall-Systeme in der Betriebsanleitung getrennt voneinander bereitgestellt.

(11) Die Hersteller stellen sicher, dass das auf dem 112-Notruf basierende bordeigene eCall-System und zusätzliche Systeme, die einen TPS-eCall-Dienst oder einen Dienst mit Zusatznutzen bereitstellen, so konzipiert sind, dass kein Austausch personenbezogener Daten zwischen den Systemen möglich ist. Wird kein System genutzt, das einen TPS-eCall-Dienst oder einen Dienst mit Zusatznutzen bereitstellt, oder verweigert die von der Datenverarbeitung betroffene Person ihre Einwilligung in die Verarbeitung ihrer personenbezogenen Daten für einen TPS-eCall-Dienst oder einen Dienst mit Zusatznutzen, darf dies keine nachteiligen Auswirkungen auf die Nutzung des auf dem 112-Notruf basierenden bordeigenen 112-eCall-Systems haben.

(12) Der Kommission wird die Befugnis übertragen, gemäß Artikel 8 delegierte Rechtsakte zu erlassen, mit denen Folgendes festgelegt wird:

a) die ausführlichen technischen Anforderungen und Prüfverfahren für die Anwendung der Vorschriften über die Verarbeitung personenbezogener Daten gemäß den Absätzen 2 und 3;

b) die ausführlichen technische Anforderungen und Prüfverfahren, mit denen sichergestellt wird, dass kein Austausch personenbezogener Daten zwischen dem auf dem 112-Notruf basierenden bordeigenen 112-eCall-System und Drittanbieter-Systemen stattfindet, wie in Absatz 11 dargelegt.

Die ersten entsprechenden delegierten Rechtsakte werden bis zum 9. Juni 2016 erlassen.

(13) Die Kommission legt im Wege von Durchführungsrechtsakten Folgendes fest:

a) die praktischen Modalitäten für die Bewertung, dass Verfolgbarkeit und Verfolgung ausgeschlossen sind, wie in den Absätzen 4, 5 und 6 dargelegt;

b) das Muster für die Nutzerinformationen gemäß Absatz 9.

Diese Durchführungsrechtsakte werden nach dem in Artikel 10 Absatz 2 genannten Prüfverfahren erlassen.

Die ersten entsprechenden delegierten Rechtsakte werden bis zum 9. Juni 2016 erlassen."

In der Verordnung wird auch darauf hingewiesen, dass es trotz des verpflichtenden Einbaus des eCall-Systems den Herstellern unbenommen bleiben soll, selbst noch eigene zusätzliche Notrufsysteme in die Kraftfahrzeuge einzubauen, wie sie auch bereits zum

jetzigen Zeitpunkt von den Herstellern angeboten werden. Dies findet in Erwägungsgrund (15) der Verordnung Berücksichtigung:

> *„Die obligatorische Ausrüstung von Fahrzeugen mit dem auf dem 112-Notruf basierenden bordeigenen eCall-System sollte das Recht aller Interessenträger, zum Beispiel von Fahrzeugherstellern und unabhängigen Anbietern, unberührt lassen, zusätzliche Notfalldienste und/oder Dienste mit Zusatznutzen parallel zu oder aufbauend auf dem auf dem 112-Notruf basierenden bordeigenen eCall-System anzubieten. Jedoch sollten diese zusätzlichen Dienste so ausgelegt sein, dass sie keine zusätzliche Ablenkung für den Fahrer bedeuten oder das Funktionieren des auf dem 112-Notruf basierenden bordeigenen eCall-Systems und die Effizienz der Arbeit der Notrufzentralen nicht beeinträchtigen. Das auf dem 112-Notruf basierende bordeigene eCall-System und das System, das private Dienste oder Dienste mit Zusatznutzen bereitstellt, sollten so konzipiert sein, dass kein Austausch personenbezogener Daten zwischen ihnen möglich ist. Wenn derartige Dienste erbracht werden, sollten sie den geltenden Sicherheits-, Sicherungs- und Datenschutzvorschriften genügen und für die Verbraucher stets optional bleiben.“*[756]

Durch Erlass der vorgenannten Verordnung wird für die Einführung des eCall-Systems eine gesetzliche Grundlage im Sinne des § 4 Abs. 1 BDSG geschaffen.

Die Zulässigkeit der Datenverwendung aus dem eCall-System bemisst sich sodann zukünftig grundsätzlich nach den Regelungen der Verordnung. Zu beachten ist jedoch, dass die Verordnung zwar bereits am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft getreten ist. Jedoch gelten die Vorschriften der Verordnung erst ab dem 31.03.2018.[757]

---

[756] Vgl. Erwägungsgrund (15) VO Nr. 2015/758, http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32015R0758&from=DE.

[757] Ausgenommen hiervon sind u.a. Art. 6 Abs. 12 und 13, die bereits ab dem 08.06.2015 gelten, vgl. Art. 14 VO Nr. 2015/758, http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32015R0758&from=DE.

Somit beurteilt sich die Zulässigkeit der Datenverwendung gemäß Art. 6, Art. 14 VO Nr. 2015/758 zum jetzigen Zeitpunkt nach den allgemeinen Grundsätzen und Erlaubnistatbeständen des Bundesdatenschutzgesetzes.[758]

Als Erlaubnistatbestand kann derzeit auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG zurückgegriffen werden. Danach ist die Datenverwendung zur Erfüllung eigener Geschäftszwecke zulässig, soweit dies zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und die schutzwürdigen Interessen des Betroffenen an dem Ausschluss der Datenverwendung nicht überwiegen. Davon ist im vorliegenden Fall insgesamt auszugehen. Denn die Lebensrettung im Notfall ist in jedem Fall als berechtigtes Interesse der verantwortlichen Stelle einzustufen. Berechtigte Interessen der verantwortlichen Stelle sind in durch die Sachlage gerechtfertigten tatsächlichen Interessen wirtschaftlicher oder ideeller Natur zu sehen, deren Verfolgung vom gesunden Rechtsempfinden gebilligt wird.[759] Dies ist in Fällen der Lebensrettung zu bejahen. Da es auch um die Rettung des Lebens des Betroffenen selbst geht, stehen auch seine schutzwürdigen Belange dem nicht entgegen. Der Betroffene kann der Verkürzung der Reaktionszeiten der Notdienste und einer Lebensrettung nach einem Unfall keine sonstigen schutzwürdigen Interessen entgegenstellen.[760] Aufgrund der Tatsache, dass insoweit ein gesetzlicher Erlaubnistatbestand greift, kommt es auf die Erteilung einer Einwilligung nicht mehr an.

Etwas anderes muss jedoch in den Fällen gelten, in denen durch das Kraftfahrzeug auch die Herz- und sonstigen Vitalfunktionen überwacht werden. Bei diesen Daten handelt es sich um besondere personenbezogene Daten im Sinne des § 3 Abs. 9 BDSG bezogen auf die Gesundheit des Betroffenen.[761] Anhand derer könnte sodann ein Profil des Betroffenen aus den ihn betreffenden besonderen personenbezogenen Daten erstellt werden. Daraus folgt, dass insoweit nur auf den Erlaubnistatbestand des § 28 Abs. 6 BDSG zurückgegriffen werden kann. Danach ist die Verwendung von solchen Gesundheitsda-

---

758 Unter Geltung des Erlaubnistatbestandes des Art. 6 sowie Erwägungsgrund (21) VO NR. 2015/758 ist insbesondere zu beachten, dass die Datenverwendung im Rahmen der Richtlinien 95/46/EG sowie 2002/58/EG erfolgt, dass die mit dem eCall-System ausgerüsteten Fahrzeuge nicht verfolgbar sind und dass keine dauerhafte Verfolgung erfolgt. Zudem muss der übermittelte Mindestdatensatz die Mindestinformationen enthalten, die für die zweckmäßige Bearbeitung von Notrufen notwendig sind. Die Zweckbestimmung zielt darauf ab, dass die nach dieser Verordnung verarbeiteten personenbezogenen Daten nur für die Handhabung in den spezifisch festgelegten Notfallsituationen verwendet werden. Die Daten sind zu löschen, sobald sie für den Zweck der Handhabung der spezifischen festgelegten Notfallsituationen nicht mehr notwendig sind.

759 Vgl. Gola/Schomerus: BDSG, [12]2015, § 28, Rn. 24.

760 Vgl. *Kremer*, RDV 2014, S. 240–252 (249).

761 Vgl. unter *Kapitel 3, Teil 2, III.2.*.

ten für eigene Geschäftszwecke nur zulässig, sofern der Betroffenen nicht eingewilligt hat und sofern er zur Erteilung der Einwilligung auch aus physischen oder rechtlichen Gründen außerstande ist.[762] Insofern ist in den Fällen, in denen das Kraftfahrzeug u.a. auch die Herzfunktion des Betroffenen erfasst, nur dann eine Datenverwendung zulässig, wenn bereits ein Notfall eingetreten ist und der Betroffene sich aus diesem Grund außerstande sieht, die Einwilligung in die Verwendung der Gesundheitsdaten selbständig zu erteilen.

2. Technische Einrichtung

An das weitere Tatbestandsmerkmal des § 87 Abs. 1 Nr. 6 BetrVG, der Überwachung durch *„technische Einrichtungen“* sind insoweit keine hohen Anforderungen zu stellen. Lediglich technische Geräte für den Alltag, wie z.B. Fernglas, Brille oder Lupe fallen aus dem Anwendungsbereich heraus.[763] Es sind bei weiter Auslegung davon alle optischen, akustischen, mechanischen sowie elektronischen Geräte umfasst.[764] Insoweit ist grundsätzlich nahezu jedes technische Gerät und dessen Einführung dazu geeignet, ein Mitbestimmungsrecht auszulösen. Aufgrund des eindeutigen Wortlauts ist allerdings die Überwachung durch einen Menschen nicht erfasst.[765]

Im vorliegenden Kontext müsste es sich bei den im Kraftfahrzeug anfallenden Daten sowie bei der Anwendung von Big Data und Telematik ebenfalls um technische Einrichtungen handeln, um hier überhaupt ein Mitbestimmungsrecht des Betriebsrates generieren zu können.

Aufgrund der Tatsache, dass es sich hier um komplexe technische Systeme handelt und insoweit auch eine Datenverwendung der daraus erzeugten Daten stattfindet, ist hier festzustellen, dass auch diese Art von Technik unter den Tatbestand des § 87 Abs. 1 Nr. 6 BetrVG zu subsumieren ist. Die Rechtsprechung des Bundesarbeitsgerichts zu diesem Tatbestandsmerkmal ist weit gefasst. Grundsätzlich sind also auch solche technischen Einrichtungen als Technik im Sinne von § 87 Abs.1 Nr. 6 BetrVG davon erfasst.

---

762 Vgl. § 28 Abs. 6 Nr. 1 BDSG.
763 Vgl. *Schwarz*: Arbeitnehmerüberwachung und Mitbestimmung, 1982, S. 95.
764 Vgl. *Klebe/Schumann*, AuR 1983, S. 40-48 (44).
765 Vgl. *Klebe* in DKKW: BetrVG, [14]2014, § 87, Rn. 168.

3. Überwachung

Es muss jedoch auch eine *„Überwachung“* vorliegen.

Als Überwachung gilt nach der Rechtsprechung des Bundesarbeitsgericht ein Vorgang, durch den Informationen über das Verhalten oder die Leistung der Arbeitnehmer erhoben und in irgendeiner Form aufgezeichnet werden, um der menschlichen Wahrnehmung zugänglich zu sein.[766] Auch die reine Auswertung von Daten ist als Überwachung einzustufen. Denn Überwachen meint sowohl das Sammeln von Informationen als auch das Auswerten von Daten im Hinblick auf bestimmte Anforderungen, die von anderen ermittelt wurden.[767]

Der letztgenannte Aspekt ist hier auch für die Anwendung von Telematik relevant. Der Versicherer erhebt dabei die Daten gerade nicht selbst, sondern lässt diese für sich aufzeichnen und in verarbeiteter Form von dem externen Dienstleister zur Verfügung stellen. Seine Tätigkeit beschränkt sich lediglich auf die Auswertung der überlassenen Score-Werte. Da eine bloße Auswertung bereitgestellter Daten jedoch in diesem Zusammenhang ausreichend ist, ist auch bei Telematik- Anwendungen von einer Überwachung im Sinne des § 87 Abs. 1 Nr. 6 BetrVG auszugehen.

Die Überwachung muss sich zudem auf das Verhalten oder die Leistung von Arbeitnehmern beziehen. Aus dem Anwendungsbereich heraus fallen dabei technische Einrichtungen, die ausschließlich reine Betriebsdaten (z.B. über Maschinennutzung, Produktion etc.) verarbeiten oder geeignet sind, der Kontrolle von Maschinen oder technischen Vorgänge zu dienen.[768] Diese lassen zunächst keine Rückschlüsse auf das Verhalten oder die Leistung von Arbeitnehmern zu. Darunter fallen insbesondere die bereits behandelten fahrzeugbezogenen Sensoren ohne Konfliktpotenzial.[769]

Hinsichtlich solcher Daten hat das Bundesarbeitsgericht bereits entschieden, dass es nicht ausreichend für die Annahme einer Überwachung sei, wenn solche Daten anhand von zusätzlichen Informationen auf den Arbeitnehmer beziehbar seien.[770]

---

766 Bundesarbeitsgericht, Beschluss vom 06.12.1983, Aktenzeichen 1 ABR 43/81, NJW 1984, S. 1476-1486 (1483).

767 Vgl. *Klebe* in DKKW: BetrVG, [14]2014, § 87, Rn. 175.

768 Vgl. *Wiese* in GK-BetrVG: Betriebsverfassungsgesetz, [10]2014, Band II, § 87, Rn. 545, 550.

769 Vgl. unter *Kapitel 2, Teil 2, I.1.a).*

770 Bundesarbeitsgericht, Beschluss vom 09.09.1975, Aktenzeichen 1 ABR 20/74, NJW 1976, S. 261-262 (262).

a) Big Data-Anwendungen

Dies muss hier jedoch mit Blick auf die derzeitigen und noch zu erwartenden technischen Möglichkeiten kritisch hinterfragt werden.

Denn durch die Anwendung von Big Data ist eine Verknüpfung sämtlicher aus dem Kraftfahrzeug zu generierender Daten möglich. Dadurch entstehen wiederum neue Datensätze, die letztlich umfassend einen Rückschluss auf den jeweiligen Arbeitnehmer als Fahrer und damit auch auf sein Verhalten und seine Leistung zulassen.[771] Es ist somit davon auszugehen, dass auf Grundlage der heutigen und noch zu erwartenden Technik regelmäßig ein Personenbezug bzw. eine Personenbeziehbarkeit hergestellt werden kann. Nach der neueren Diktion des Bundesarbeitsgerichts liegen sodann *„individualisierte oder individualisierbare Verhaltens- oder Leistungsdaten“* vor.[772] Die Verknüpfung der Daten und deren Auswertung erfordert dabei keinen erheblichen Aufwand. Im Gegenteil ist es bereits mit relativ wenig Zeit- und Arbeitsaufwand möglich, sämtliche bereits erhobenen und gespeicherten Daten nach neuen Mustern miteinander zu verknüpfen und wiederum auszuwerten. Diese niedrige Schwelle, die mittlerweile anzusetzen ist, um einen Personenbezug bzw. eine Personenbeziehbarkeit herstellen zu können, muss hier besondere Berücksichtigung finden.

Insoweit müssen die Grundsätze der vorgenannten Rechtsprechung in Bezug auf die sich aus der Vernetzung der Kraftfahrzeuge ergebenden Möglichkeiten modifiziert werden. Aufgrund der Tatsache, dass dabei eine Verknüpfung und weitere Auswertung der Daten relativ einfach möglich ist, muss dies hier im Hinblick auf die dadurch entstehenden Gefahren für das Persönlichkeitsrecht des Betroffenen als Überwachung der Leistung und des Verhaltens der Arbeitnehmer eingestuft werden.

Besonders problematisch erscheint in Bezug auf Big Data-Anwendungen die Zweckbindung der Datenverarbeitung. Denn jede einzelne Datenverarbeitung muss bereits an dem datenschutzrechtlichen Grundprinzip der Zweckbindung gemessen werden.[773] Werden nunmehr einzelne Daten über Big Data-Anwendungen miteinander verknüpft, muss für die daraus gewonnenen neuen Datensätze ebenfalls der Grundsatz der Zweckbindung eingehalten werden. Dies erscheint aufgrund der vielfältigen Möglichkeiten,

---

771 Vgl. unter *Kapitel 2, Teil 5, II.*.

772 Bundesarbeitsgericht, Beschluss vom 25.09.2012, Aktenzeichen 1 ABR 45/11, NZA 2013, S. 275-277 (276).

773 Vgl. unter *Kapitel 3, Teil 2, I.5.*.

die sich aus einem aus Datenverknüpfung resultierenden Datensatz und dessen Verwendung, insbesondere auch aufgrund der technisch bestehenden Möglichkeiten ergeben können, problematisch. Für jeden neuen Datensatz ist es erforderlich, dass auch dieser einen bestimmten Zweck verfolgt, der sich eindeutig aus der Datenverarbeitung ergeben muss.

Dies wird die Verantwortlichen einer Verarbeitung von Daten aus dem vernetzten Fahrzeug vor eine Herausforderung stellen, da eine eindeutige Zweckbindung nicht erkennbar sein wird. Dies und eine diesbezüglich eindeutige Erklärung wären jedoch Voraussetzung, um beispielsweise eine wirksame Einwilligung des betroffenen einholen zu können. Dazu wird es jedoch auch auf die weiteren technischen Entwicklungen und deren Anwendung ankommen.

b) Praktischer Anwendungsfall: Intelligente Verkehrssteuerung

Ein praktischer Anwendungsfall einer Überwachung durch Big Data-Anwendung kann in Bezug auf die Technik vernetzter Fahrzeuge insbesondere im Bereich der intelligenten Verkehrssteuerung gesehen werden. Die intelligente Verkehrssteuerung wird dabei insbesondere verwirklicht durch die Anwendung von Verkehrstelematik.[774]

(i) Szenarien

Die Verkehrstelematik soll sich zukünftig derart entwickeln, dass es möglich sein wird, Kraftfahrzeuge mit straßenseitig installierten Anlagen wie beispielsweise Ampelanlagen derart zu verbinden, dass sich daraus eine Verkehrsoptimierung ergibt. Denkbar ist dabei, dass die Ampelsignale mit den aus dem Kraftfahrzeug vorhandenen Daten verbunden werden. Durch Verknüpfung dieser Daten mit den Geschwindigkeitsdaten und den GPS-Daten aus dem Kraftfahrzeug könnte sodann errechnet und dem Fahrer mittels Anzeige mitgeteilt werden, welche Geschwindigkeit angemessen ist, um die Grünphase einer Ampel noch zu erreichen. Durch die Geschwindigkeitsdaten könnte in Verbindung mit den Positionsdaten des Kraftfahrzeugs die Entfernung zur Ampelanlage berechnet werden.[775] Zusätzlich könnte eine Verknüpfung mit den Schaltzeiten der Ampelanlage stattfinden, sodass anhand dieser Angaben zusammen mit Daten über etwaige Verkehrshindernissen eine für den Fahrer verlässliche Angabe dazu geliefert werden könnte, wie lange die Grünphase noch andauert, ob diese von ihm überhaupt noch zu errei-

774 Vgl. auch unter *Kapitel 2, Teil 4*.
775 Vgl. *Kremer*, RDV 2014, S. 240–252 (248).

chen wäre und mit welcher Geschwindigkeit er in letzterem Fall fahren müsste, um die Grünphase noch nutzen zu können. Dazu wurden bereits entsprechende Systeme entwickelt. Das System *„eHorizon“* beispielsweise gibt dem Fahrer ein Signal, wenn die Ampel auf Rot umschaltet und lässt den Wagen automatisch ausrollen, was Wartezeiten verhindern und den Benzinverbrauch senken soll.[776] Dies ist der typische Fall optimierender und intelligenter Verkehrssteuerung.

Aber auch andere Daten, die im Rahmen der Verkehrstelematik und dabei insbesondere durch Car to Car und Car to Infrastructure anfallen und generiert werden, könnten zur adaptiven Verkehrssteuerung genutzt werden. Über sog. Roadside Units werden die Daten von Ampelanlagen und Straßenzuständen zusammen mit den Daten aus den im Umkreis befindlichen Kraftfahrzeugen gesammelt und ausgewertet.[777] Zur Unfallvermeidung können auch die Daten aus dem Kraftfahrzeug zu Temperatur und Regensensor sowie zur etwaig eingeschalteten Warnblinkanlage genutzt werden, um andere Verkehrsteilnehmer über bestehende Gefahren zu warnen.

Beispielhaft soll für die Umsetzung dieser Maßnahmen der Aufbau des sog. Mobilitäts Daten Marktplatzes[778] angeführt werden. Es handelt sich dabei um ein zweistufiges System. Verkehrsdaten können darüber einfach und unkompliziert zwischen Datenanbietern und Datenabnehmern ausgetauscht werden. Beteiligt sind dabei insbesondere die öffentliche Hand sowie private Dienstanbieter.[779] Auf der ersten Stufe können über das bereitgestellte Portal[780] Daten von Nutzern angeboten und beworben werden. Es ist darüber möglich, Kontakt zu möglichen Abnehmern und Interessenten in Bezug auf die Verkehrsdaten herzustellen. Auf der zweiten Stufe werden die entsprechenden Daten sodann an den Datenabnehmer übertragen. Die Übertragung erfolgt in standardisierten Formaten. So ist es möglich, über das entsprechende Portal verkehrsrelevante Daten anzubieten, zu suchen und zu abonnieren. Dies führt wiederum dazu, dass die Verkehrsdaten bestmöglich genutzt und ausgetauscht werden können, was letztlich zu einer verbesserten Verkehrssteuerung beitragen soll.

---

776 Vgl. *Stephan*, BILD, 15.06.2015, S. 10.
777 Vgl. unter *Kapitel 2, Teil 4, II.3.*.
778 Vgl. unter *Kapitel 2, Teil 4, II.3*. sowie http://www.mdm-portal.de/.
779 Vgl. http://www.bmvi.de/DE/VerkehrUndMobilitaet/DigitalUndMobil/MDM/mdm_node.html.
780 Vgl. http://www.mdm-portal.de/.

(ii) Rechtliche Würdigung

Die Übertragung der vorgenannten verschiedenen Daten zur Optimierung der Verkehrssicherheit und der Verkehrssteuerung ist ausschließlich im Falle der vollständigen Anonymisierung rechtlich nicht zu beanstanden und stellt für diesen Fall keine weiteren Anforderungen an die datenschutzrechtliche Ausgestaltung.

Erfolgt allerdings keine Anonymisierung, handelt es sich bei den übertragenen Daten auch um personenbezogene bzw. personenbeziehbare Daten, bei deren Vorliegen die Schutzmechanismen des Bundesdatenschutzgesetzes greifen. Insbesondere am Beispiel der vorgenannten Verknüpfung der Daten aus dem Kraftfahrzeug mit den Daten der Ampelanlage wird deutlich, dass dadurch Dritten die Möglichkeit eröffnet wird, umfassende Verhalts- und Bewegungsprofile des Fahrers zu erstellen. Dies wird vor allem relevant, wenn dem Fahrer beispielsweise angezeigt wird, dass die Grünphase von ihm nicht mehr zu erreichen ist und dieser daraufhin trotzdem beschleunigt und im Zweifel einen Rotlichtverstoß begeht. Dieser wäre anhand der Daten nachweisbar. Dies führt unter Umständen zu eine schwerwiegenden Eingriff in das allgemeine Persönlichkeitsrecht des Betroffenen.

Ein diese Datenverwendung zulassender Erlaubnistatbestand ist dafür nicht gegeben. Insbesondere kann die Datenverwendung durch Dritte im Rahmen eines bestehenden Arbeitsverhältnisses nicht über den Erlaubnistatbestand des § 32 BDSG gerechtfertigt werden. Diese Art der Datenverwendung ist nicht erforderlich zur Durchführung des Arbeitsverhältnisses. Eine solche Zwecksetzung würde über das erforderliche Maß hinausgehen.

Auch aus den Vorschriften des Intelligente Verkehrssysteme Gesetzes kann keine Erlaubnisnorm abgeleitet werden, die als *„andere Rechtsvorschrift“* im Sinne des § 4 Abs. 1 BDSG ebenfalls zu berücksichtigen wäre.[781] Zudem verfügen diese Vorschriften nicht über die notwendige Regelungstiefe und Normenklarheit.[782]

Gemäß § 4 Abs. 1 BDSG müsste in diesem Fall mangels eines gesetzlichen Erlaubnistatbestandes auf die Einwilligung des Betroffenen abgestellt werden, um von einer zulässigen Datenverwendung sprechen zu können. Die Datenverwendung im Rahmen

781 Vgl. unter *Kapitel 3, Teil 3, I.2.b).*
782 Vgl. *Lüdemann/Sengstacken*, RDV 2014, S. 177–182 (180).

intelligenter Verkehrssysteme kann mithin nur durch Erteilung einer wirksamen Einwilligung seitens des Betroffenen Fahrers umgesetzt werden.

Zudem ist in diesem Fällen das aufgrund der Überwachung des Arbeitnehmers durch technische Einrichtungen bestehende Mitbestimmungsrecht des Betriebsrates nach § 87 Abs. 1 Nr. 6 BetrVG zu beachten. Sofern die Daten aus einem Dienstfahrzeug im Rahmen der intelligenten Verkehrssysteme übertragen werden, muss hier von einer Überwachung des Verhaltens und der Leistung des Arbeitnehmers ausgegangen werden.

c) Praktischer Anwendungsfall: Regressansprüche des Arbeitgebers

Ein weiterer praktischer Anwendungsfall, der den Tatbestand der *„Überwachung“* im Sinne des § 87 Abs. 1 Nr. 6 BetrVG erfüllt, ist in Regressansprüche des Arbeitgebers gegenüber dem Arbeitnehmer für den Fall, dass der Arbeitnehmer mit dem ihm überlassenen Dienstfahrzeug einen Unfall verursacht oder es aufgrund Unachtsamkeit des Arbeitnehmers zu Sachschaden am Kraftfahrzeug kommt, zu sehen.

(i) Szenarien

Der Arbeitgeber wird zukünftig immer mehr dazu in der Lage sein, anhand der im Kraftfahrzeug eingebauten Technik seine Arbeitnehmer, denen ein Dienstfahrzeug zur dienstlichen und eventuell privaten Nutzung überlassen wurde, zu überwachen. Dadurch könnte es ihm ermöglicht werden, beispielsweise anhand der durch den Einbau und die Verwendung einer Telematik-Box generierten Daten Informationen zum Fahrverhalten des jeweiligen Arbeitnehmers zu erhalten. Selbst für den Fall, dass diese ihm von einem Dienstleister nur als Score-Werte überlassen werden[783], ist regelmäßig trotz alledem ein Rückschluss auf das Fahrverhalten möglich. Durch die Verknüpfung dieser Daten mit GPS-Daten, Standortdaten sowie Daten aus verschiedenen fahrzeug- und fahrerbezogenen Sensoren lässt sich seitens des Arbeitgebers ein Profil über den fahrenden Arbeitnehmer erstellen. Aus all diesen Daten könnten sich Erkenntnisse darüber ergeben, wann der Arbeitnehmer als Betroffener das Fahrzeug genutzt hat, welche Wetterverhältnisse vorlagen, wie schnell er gefahren ist und ob es sich dabei um eine Privatfahrt oder einen dienstlichen Auftrag handelte. Anhand dessen könnte der Arbeitgeber nachvollziehen, ob das Kraftfahrzeug während der Arbeitszeit genutzt wurde und ob der Arbeitnehmer die ihn treffende Sorgfaltspflicht angemessen ausgeübt hat.

---

783 Vgl. unter *Kapitel 2, Teil 5, II.*.

Verursacht der Arbeitnehmer mit dem ihm überlassenen Kraftfahrzeug einen Unfall, könnte anhand der vorliegenden Daten analysiert werden, ob der Unfall eventuell auf grobe Fahrlässigkeit des Arbeitnehmers zurückzuführen ist, weil dieser die vorgeschriebene Höchstgeschwindigkeit z.B. bei schlechten Witterungsverhältnissen überschritten hat und deshalb die Kontrolle über das Fahrzeug verlor. Sofern eine daraus resultierende Beschädigung ebenfalls noch außerhalb der Arbeitszeit verursacht wird, hat der Arbeitgeber ein Interesse daran, den Vorfall aufzuklären, um die ihm zustehenden Ansprüche gegen den Arbeitnehmer durchsetzen zu können.

(ii) Rechtliche Würdigung

Den Arbeitnehmer trifft zunächst im Hinblick auf das ihm überlassene Dienstfahrzeug als Arbeitgebereigentum eine Sorgfaltspflicht, insbesondere für den Fall einer gestatteten Privatnutzung.[784] Er ist verpflichtet, mit den Einrichtungen und Arbeitsmitteln des Betriebs sorgfältig umzugehen.[785]

Sollte dies nicht der Fall sein, kann der Arbeitgeber Regressansprüche gegen den Arbeitnehmer aus einem der vorgenannten Szenarien über die Grundsätze zum innerbetrieblichen Schadensausgleich geltend machen.[786] Grundsätzlich haftet auch der Arbeitnehmer für Vorsatz und Fahrlässigkeit im Sinne des § 276 BGB mangels spezialgesetzlicher Regelungen nach den allgemeinen Vorschriften und sieht sich somit Schadensersatzansprüchen nach §§ 280 ff, 823 BGB ausgesetzt. Die Frage, ob der Arbeitnehmer die Pflichtverletzung im Sinne des § 280 Abs. 1 BGB zu vertreten hat, ist an den Vorgaben in § 619a BGB abweichend von § 280 Abs. 1 Satz 2 BGB zu messen.[787] Die Beschränkung der Arbeitnehmerhaftung gilt dabei für alle Arbeiten, die durch den Betrieb veranlasst sind und aufgrund eines Arbeitsverhältnisses geleistet werden, auch wenn diese Arbeiten nicht gefahrgeneigt sind.[788] Die Haftung ist in diesen Fällen entsprechend § 254 BGB beschränkt.[789]

---

784 Vgl. *Jaspers/Franck*, RDV 2015, S. 69–73 (72).

785 Vgl. *Müller-Glöge* in Säcker/Rixecker/Oetker: MüKo BGB, Band 4, ^{6}2012, § 611, Rn. 1082.

786 An dieser Stelle soll jedoch lediglich der Fall einer Schädigung des Arbeitgebers an dessen Rechtsgütern untersucht werden. Die Fälle der Schädigung anderer Arbeitnehmer bleiben unberücksichtigt.

787 Vgl. *Brors* in Hümmerich/Boecken/Düwell: Arbeitsrecht, Band 1, ^{2}2010, § 611 BGB, Rn. 877.

788 Großer Senat des Bundesarbeitsgerichts, Beschluss vom 27.09.1994, Aktenzeichen GS 1/89 (A), NJW 1995, S. 210-213.

789 Bundesarbeitsgericht, Urteil vom 18.01.2007, Aktenzeichen 8 AZR 250/06, NZA 2007, S. 1230-1235.

Voraussetzung dafür ist jedoch das Vorliegen einer betrieblich veranlassten Tätigkeit. Es muss sich dabei um eine unmittelbar betrieblich veranlasste Tätigkeit handeln, die im Interesse des Betriebs vorgenommen wird. Unmittelbar betrieblich veranlasst ist jede arbeitsvertraglich geschuldete Tätigkeit, wobei es lediglich darauf ankommt, ob die Tätigkeit betrieblich veranlasst ist, während die konkrete Ausführung der Tätigkeit durch den Arbeitnehmer im Rahmen des Eigenverschuldens zu prüfen ist.[790] Die schadensverursachende Tätigkeit muss im Interesse des Betriebs liegen. Dieses Merkmal ist von Relevanz, wenn es sich um eine betriebsbezogene Tätigkeit außerhalb des eigentlichen Aufgabenbereichs des Arbeitnehmers handelt. In diesen Fällen kommt es maßgeblich darauf an, ob der Arbeitnehmer seine Tätigkeit für zweckmäßig halten durfte.[791] Die Grundsätze über die Beschränkung der Haftung des Arbeitnehmers bei betrieblich veranlassten Tätigkeiten sind zudem einseitig zwingendes Arbeitnehmerschutzrecht, von welchem weder einzel- noch kollektivvertraglich zu Lasten des Arbeitnehmers abgewichen werden kann.[792] Unzulässig sind somit in Arbeitsverträgen oder Betriebsvereinbarungen vereinbarte Bestimmungen, die zu Lasten des Arbeitnehmers von den Grundsätzen der eingeschränkten Arbeitnehmerhaftung abweichen und insbesondere eine Haftungsverschärfung vorsehen.[793]

Die Haftungsbeschränkung führt dazu, dass eine volle Haftung des Arbeitnehmers nur bei Vorsatz und bei Fahrlässigkeit besteht, soweit im Falle letzterer die Schadensersatzpflicht den Arbeitnehmer in seiner wirtschaftlichen Existenz gefährdet, während bei mittlerer Fahrlässigkeit eine Aufteilung des Schadens zwischen Arbeitnehmer und Arbeitgeber im Rahmen einer Abwägung der Gesamtumstände vorgenommen wird und bei leichtester Fahrlässigkeit die Haftung des Arbeitnehmers gänzlich ausgeschlossen ist.[794]

Im vorliegenden Zusammenhang ist die schadensgeneigte Tätigkeit im Führen des Dienstfahrzeugs durch den Arbeitnehmer zu sehen. Wird dabei ein Unfall verursacht oder ein Rechtsgut des Arbeitgebers beschädigt, dienen die Grundsätze des innerbe-

---

790 Vgl. *Reichold* in Richardi/Wlotzke/Wißmann/Oetker: Mü-HB Arbeitsrecht, Band 1, ^{3}2009, § 51, Rn. 32.

791 Bundesarbeitsgericht, Urteil vom 02.03.1971, Aktenzeichen VI ZR 146/69, AP RVO § 637 Nr. 6.

792 Bundesarbeitsgericht, Urteil vom 05.02.2004, Aktenzeichen 8 AZR 91/03, NJW 2004, S. 2469-2471

793 Vgl. *Lakies* in Kittner/Zwanziger/Deinert: Arbeitsrecht, ^{7}2013, § 62, Rn. 27a.

794 Vgl. *Weidenkaff* in Palandt/Bassenge: BGB-Kommentar, ^{74}2014, § 611, Rn. 157a.

trieblichen Schadensausgleichs dazu, festzustellen, ob der Arbeitnehmer in dem jeweiligen Einzelfall zur Haftung herangezogen werden kann.

Um die Voraussetzungen für den innerbetrieblichen Schadensausgleich beweisen zu können, könnten insoweit auf die Daten aus dem Kraftfahrzeug zugegriffen werden. Notwendig ist hierbei jedoch eine Differenzierung danach, ob es sich um eine rein dienstliche Nutzung des Kraftfahrzeugs handelt oder ob dem Arbeitnehmer auch die private Nutzung desselben erlaubt ist.

Handelt es sich bei dem Gebrauch des Kraftfahrzeugs durch den Arbeitnehmer um eine rein dienstliche Nutzung, kann für die Datenverwendung auf den Erlaubnistatbestand des § 32 Abs. 1 BDSG zurückgegriffen werden, sofern die Nutzung des Kraftfahrzeugs eng mit dem übrigen Pflichtenkreis des Arbeitnehmers verknüpft ist, weil dieser beispielsweise als Kurier- oder Berufskraftfahrer arbeitet.[795] In diesen Fällen stellt das Kraftfahrzeug das Hauptarbeitsmittel des Arbeitnehmers dar. Eine Nutzung des Kraftfahrzeugs ist in diesen Konstellationen zwingend notwendig, um die geschuldete Arbeitsleistung ordnungsgemäß erbringen zu können. Dieser Aspekt dient letztlich ebenfalls der Rechtfertigung der Datenverwendung durch den Arbeitgeber. Denn dieser hat ein Interesse daran, diese Informationen zu erhalten. Die vom Arbeitnehmer erbrachte Fahrleistung dient der Durchführung des Beschäftigungsverhältnisses zumindest bei Berufskraftfahrern und führt dazu, dass es dem Arbeitgeber erlaubt sein muss, diesem Zweck entsprechend Kontrollen durchzuführen. Es besteht insoweit ein Beweggrund zur Datenverwendung. Sofern im Zusammenhang mit einer rein dienstlichen Nutzung also das Kraftfahrzeug beschädigt wird, kann eine Datenverwendung nach dem Erlaubnistatbestand des § 32 BDSG zulässig sein.

Anders stellt sich dies bei einer auch privaten Nutzung des Dienstfahrzeugs dar. Grundsätzlich muss eine etwaige Datenverwendung seitens des Arbeitgebers auf die Arbeitszeit beschränkt bleiben. Fahrten außerhalb der Arbeitszeit lassen sich nicht mehr mit dem Zweck der Durchführung des Beschäftigtenverhältnisses rechtfertigen. Dies betrifft insoweit eine Rechtfertigung der Datenverwendung in Bezug auf Privatfahrten gemäß § 32 BDSG.

795 Vgl. *Jaspers/Franck*, RDV 2015, S. 69–73 (72).

Jedoch ist zu beachten, dass die Datenverwendung darüber hinaus allerdings nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG erlaubt sein kann, sofern der Arbeitgeber vertragliche Ansprüche geltend machen will.[796] Denkbar ist dies insbesondere für die Fälle, in denen der Arbeitgeber Anhaltspunkte dafür hat, dass eine Beschädigung des Kraftfahrzeugs auf eine sorgfaltswidrige Privatnutzung des Kraftfahrzeugs zurückzuführen ist.[797] Sodann könnte der Arbeitgeber diese Ansprüche im Rahmen des Beschäftigungsverhältnisses geltend machen und zu Beweiszwecken auf die Daten aus dem Kraftfahrzeug zurückgreifen und diese Datenverwendung nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG rechtfertigen. Dies dient in diesem Zusammenhang der Durchführung des Beschäftigungsverhältnisses.

Für den Fall einer unzulässigen Datenverwendung zu Beweiszwecken in einem Haftungsprozess sind eventuell bestehende Beweiserhebungs- und Beweisverwertungsverbote zu beachten.[798] Auch in diesem Fall ist jedoch letztlich ein Mitbestimmungsrecht des Betriebsrates nach § 87 Abs. 1 Nr. 6 BetrVG zu beachten.

4. Außerbetriebliches Verhalten

Diskutiert wird auch die Frage, wie das Verhalten von Arbeitnehmern außerhalb der Arbeit zu qualifizieren ist. Nach *Müllner* soll bereits das Verkehrsverhalten auf dem Firmengelände nicht mehr als Verhalten des Arbeitnehmers im Sinne von § 87 Abs. 1 Nr. 6 BetrVG eingestuft werden, da kein Überwachungsdruck entstehe.[799]

Dieser Auffassung steht jedoch die herrschende Meinung in der Literatur entgegen.[800] Danach sollen auch außerbetriebliche Verhaltensweisen Berücksichtigung finden als Verhalten des Arbeitnehmers im Sinne des § 87 Abs. 1 Nr. 6 BetrVG. Es soll keine Beschränkung auf das Verhalten bei der Arbeit geben.

Letztgenannter Auffassung ist hier zuzustimmen. Denn bereits aus dem Wortlaut lässt sich eine solch enge Auslegung, wie sie *Müllner* vertritt, nicht ableiten. Im Gegensatz

---

796 Zum Verhältnis der Vorschrift des § 32 BDSG zu der Regelung des § 28 BDSG vgl. unter *Kapitel 3, Teil 3, I.1.c)(i).*

797 So *Jaspers/Franck*, RDV 2015, S. 69–73 (73).

798 Diese werden im Umfang der vorliegenden Untersuchung nicht näher dargestellt.

799 Vgl. *Müllner*, DB 1984, S. 1677-1680 (1678).

800 Vgl. *Klebe*, DB 1986, S. 380-382 (380); *Hinrichs*, AuR 1986, S. 285-288 (288); *Ehmann*, ZfA 1986, S. 357-401 (371); *Schwarz*, BB 1985, S. 531-535 (532); *Wiese* in GK-BetrVG: Betriebsverfassungsgesetz, [10]2014, Band II, § 87, Rn. 540; *Klebe* in DKKW: BetrVG, [14]2014, § 87, Rn. 181; *Fitting*: Betriebsverfassungsgesetz, [27]2014, § 87, Rn. 221.

zu dem Tatbestand des § 87 Abs. 1 Nr. 1 BetrVG *(„Verhalten der Arbeitnehmer im Betrieb")* findet sich eine solche Einschränkung in dem hier relevanten Tatbestand des § 87 Abs. 1 Nr. 6 BetrVG gerade nicht. Auch könne der Arbeitnehmer unter Umständen sogar besser geschützt sein, wenn auch das Verhalten in Pausen oder die Freizeitgestaltung für ein Mitbestimmungsrecht ebenfalls zu beachten wäre.[801] Zudem würde eine Differenzierung hier zu widersprüchlichem Verhalten seitens des Arbeitgebers führen, wenn dieser einerseits die sich aus dem Verhalten des Arbeitnehmers außerhalb des Betriebs bzw. der Arbeit generierbaren Daten zwar speichern bzw. auswerten, andererseits jedoch ein Mitbestimmungsrecht des Betriebsrates mit der Begründung ablehnen wollte, dies sei nicht vom Tatbestand umfasst.[802]

Aufgrund dessen muss hier für die Prüfung, ob ein Mitbestimmungsrecht besteht, jedes Verhalten eines Arbeitnehmers berücksichtigt werden, das im Zusammenhang mit der Ausführung des Arbeitsverhältnisses steht. Dies wird auch durch die Rechtsprechung des Bundesarbeitsgerichts gefestigt. In der Entscheidung Opel-PAISY vom 11.03.1986[803] bestätigte das Bundesarbeitsgericht, dass für die Entscheidung über ein Mitbestimmungsrecht des Betriebsrates jedes personenbezogene Datum heranzuziehen sei. Es komme nicht darauf an, ob Daten im Einzelnen eine Aussage über Verhalten oder Leistung des Arbeitnehmers geben würden.

Diese Auslegung spielt für die vorliegende Untersuchung eine gewichtige Rolle. Denn vielfach wird der Arbeitnehmer ein im Eigentum des Arbeitgebers stehendes und ihm auch zum privaten Gebrauch überlassenes Kraftfahrzeug tatsächlich auch privat nutzen. Somit auch in seiner Freizeit. Unabhängig von der datenschutzrechtlichen Relevanz muss hier ein Mitbestimmungsrecht des Betriebsrates bejaht werden. Denn auch aus dem Verhalten des Arbeitnehmers während der Freizeit lassen sich Rückschlüsse auf die Persönlichkeit des Arbeitnehmers ziehen. Aufgrund der Tatsache, dass in technischer Hinsicht in den meisten Fällen bei der Speicherung der Daten nicht zwischen Arbeitszeit und Freizeit unterschieden wird, kann ohnehin keine saubere Trennung beider Bereiche erfolgen. Es muss insoweit tatsächlich jedes Datum relevant sein, welches letztlich einen Personenbezug bzw. eine Personenbeziehbarkeit aufweist.

---

801 Vgl. *Klebe*, DB 1986, S. 380-382 (381)

802 Vgl. *Hinrichs*, AuR 1986, S. 285-288 (288)

803 Bundesarbeitsgericht, Beschluss vom 11.03.1986, Aktenzeichen 1 ABR 12/84, NZA 1986, S. 526-530.

Gleiches gilt auch für die Anwendungen von Telematik und Big Data. Dabei werden ebenfalls Verhaltensweisen des Arbeitnehmers erfasst, die nicht in direktem Zusammenhang mit dem Arbeitsverhältnis stehen, die aber gleichfalls dem Arbeitgeber im Zweifel ebenfalls zur Verfügung stehen. Dadurch ergeben sich zusätzliche Kontrollmöglichkeiten für den Arbeitgeber. Dies rechtfertigt es, auch insoweit von einer Überwachung auszugehen. Es muss deshalb auch ein solches Verhalten Berücksichtigung finden mit der Konsequenz, dass dabei eine Überwachung des Verhaltens oder der Leistung des Arbeitnehmers nach § 87 Abs. 1 Nr. 6 BetrVG stattfindet.

5. Zur Überwachung bestimmt

Die technische Einrichtung muss zur Überwachung bestimmt sein.

Zur Überwachung *"bestimmt"* sind technische Einrichtungen dann, wenn sie objektiv geeignet sind, Verhaltens- oder Leistungsinformationen der Arbeitnehmer zu erheben und aufzuzeichnen, sodass es auf die subjektive Überwachungsabsicht des Arbeitgebers nicht ankommt.[804] Objektiv zur Überwachung geeignet sind solche technischen Einrichtungen, die aufgrund des verwendeten Programms Verhaltens- und Leistungsdaten erfassen und aufzeichnen, auswerten oder durch Verarbeitung der Daten Aussagen über Verhalten oder Leistung gewonnen werden.[805]

Das Bundesarbeitsgericht hat in seiner früheren Rechtsprechung bereits darauf abgestellt, dass die technische Einrichtung selbst die Überwachung bewirken muss.[806] Mit der Entscheidung des Bundesarbeitsgerichts zum *„Routenplaner“* vom 10.12.2013[807] wurde dieses Erfordernis abermals aufgegriffen. Die technische Einrichtung müsse aufgrund ihrer technischen Natur unmittelbar, das heißt wenigstens in ihrem Kern die Überwachung vornehmen, indem sie das Verhalten oder die Leistung der Arbeitnehmer kontrolliere. Das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG setze daher voraus, dass die technische Einrichtung selbst und automatisch die Daten über bestimmte

---

804 Bundesarbeitsgericht, Beschluss vom 10.12.2013, Aktenzeichen 1 ABR 43/12, DuD 2014, S. 633-634 (633).

805 Vgl. dazu *Klebe* in DKKW: BetrVG, [14]2014, § 87, Rn. 186 sowie Bundesarbeitsgericht, Beschluss vom 06.12.1983, Aktenzeichen 1 ABR 43/81, NJW 1984, S. 1476-1486 (1483); Bundesarbeitsgericht, Beschluss vom 14.09.1984, Aktenzeichen 1 ABR 23/82, NJW 1985, S. 450-453 (451); Bundesarbeitsgericht, Beschluss vom 11.03.1986, Aktenzeichen 1 ABR 12/84, NZA 1986, S. 526-530 (527).

806 Bundesarbeitsgericht, Beschluss vom 08.11.1994, Aktenzeichen 1 ABR 20/94, NZA 1995, S. 313-314 (313).

807 Bundesarbeitsgericht, Beschluss vom 10.12.2013, Aktenzeichen 1 ABR 43/12, DuD 2014, S. 633-634.

Vorgänge verarbeitet.[808] Dies sei bei einem Routenplaner jedoch nicht der Fall. Es handele sich bei dem Routenplaner, ebenso wie beispielsweise bei einem Taschenrechner, nur um eine Entscheidungshilfe, die lediglich Hilfsfunktion erfülle.[809] Insoweit ist zwar nach der Rechtsprechung des Bundesarbeitsgerichts tatsächlich darauf abzustellen, ob die technische Einrichtung selbst die Überwachung bewirkt. Das ist jedoch nur der Fall, wenn dies über eine Entscheidungshilfe hinausgeht. Im Gegensatz zum Routenplaner sei dieses Ergebnis allerdings für GPS-Systeme anzunehmen, die Informationen über das Fahrverhalten aufzeichnen und deshalb als mitbestimmungspflichtig einzustufen seien.[810]

a) Überwachung bei Big Data-Anwendung

Eine Einschränkung für Anwendungen von Big Data und Telematik könnte sich gerade daraus ergeben, dass es sich bei den Anwendungen um eine *„Überwachung“* handelt. Dies könnte hier problematisch sein in der Hinsicht, dass die Daten daraus nicht von sich aus bereits zur Überwachung des Arbeitnehmers bestimmt sind.

Allerdings vertritt das Bundesarbeitsgericht seit der Entscheidung zum *„Technikerberichtssystem“*[811] eine weitgehende Auffassung.[812] Es kommt also nicht darauf an, ob die Daten beispielsweise manuell erhoben und danach nur gespeichert werden. Vielmehr reicht es aus, wenn die entsprechende Verwendung als Teil eines mehrstufigen Vorgangs der Überwachung[813] anzusehen ist. Zudem ist es bei der Anwendung von Big Data und Telematik eindeutig, dass die Daten dort auf technischem Wege erhoben werden und nicht auf manuelle Art und Weise, sodass dies den technischen Charakter nochmals festigt. Insoweit fallen auch solche neuen Technikanwendungen unter den Tatbestand des § 87 Abs. 1 Nr. 6 BetrVG.

---

808 Bundesarbeitsgericht, Beschluss vom 10.12.2013, Aktenzeichen 1 ABR 43/12, DuD 2014, S. 633-634 (633); Bundesarbeitsgericht, Beschluss vom 08.11.1994, Aktenzeichen 1 ABR 20/94, NZA 1995, S. 313-314 (313).

809 So *Däubler*: Gläserne Belegschaften, ^{6}2015, Rn. 757a.

810 Bundesarbeitsgericht, Beschluss vom 10.12.2013, Aktenzeichen 1 ABR 43/12, DuD 2014, S. 633-634 (633).

811 Bundesarbeitsgericht, Beschluss vom 14.09.1984, Aktenzeichen 1 ABR 23/82, NJW 1985, S. 450-453.

812 Bundesarbeitsgericht, Beschluss vom 23.04.1985, Aktenzeichen 1 ABR 2/82, NZA 1985, S. 671-673; Bundesarbeitsgericht, Beschluss vom 11.03.1986, Aktenzeichen 1 ABR 12/84, NZA 1986, S. 526-530.

813 Vgl. *Schwarz*, BB 1985, S. 531-535 (531).

Von einer Überwachung des Arbeitnehmerverhaltens ist dabei insbesondere auszugehen, wenn durch Anwendung von GPS oder anderer geeigneter Anwendungen Positionsdaten übermittelt werden. Dies führt dazu, dass dadurch das Bewegungsverhalten des Arbeitnehmers überwacht werden kann. Durch die sodann vorliegenden Positionsdaten lässt sich nachvollziehen, wann sich ein externer Arbeitnehmer an welchem Ort aufgehalten hat. Es ist selbst in den Fällen von einer Überwachung im Sinne des § 87 Abs. 1 Nr. 6 BetrVG auszugehen, in denen sich solche Positionsdaten über das Bewegungsverhalten des Arbeitnehmers nur als Nebeneffekt der Nutzung der technischen Einrichtung zeigt. Es ist lediglich für die Annahme einer Überwachung erforderlich, dass gegebenenfalls auch weitere Mittel notwendig sind, um an die Daten zu gelangen. Dies hat das Bundesarbeitsgericht bereits festgestellt:

> *„Unmittelbar geeignet ist eine technische Einrichtung nur dann nicht, wenn sie allein - ohne Hinzutreten weiterer Mittel - noch keine (verwertbaren) Überwachungsergebnisse liefert."*[814]

Im Umkehrschluss reicht es somit aus, wenn sich die Überwachungsergebnisse aus den sich aus der technischen Einrichtung ergebenden Daten unter Hinzuziehung weiterer Mittel generieren lassen. Sofern die Überwachungsergebnisse also nur Nebeneffekt sind, sind auch sie als geeignet im Sinne der Vorschrift anzusehen, um eine Überwachung des Arbeitnehmerverhaltens auszugehen.

Hinsichtlich solcher Überwachungsmaßnahmen kann auf die Grundsätze zur Videoüberwachung zurückgegriffen werden.[815] Ebenso wie die Überwachung am Arbeitsplatz durch den Einsatz von Videokameras muss auch eine Überwachung mittels anderer technischer Geräte, wie z.B. eine Standortermittlung via GPS streng limitiert werden und einer strengen Zweckbindung unterliegen. Eine Regelung zur Videoüberwachung in öffentlich zugänglichen Räumen existiert in Gestalt der Vorschrift des § 6b BDSG[816].

---

814 Bundesarbeitsgericht, Beschluss vom 10.07.1979, Aktenzeichen 1 ABR 50/78, DB 1979, S. 2428-2429.

815 Vgl. auch unter *Kapitel 3, Teil 7, III.2.*.

816 Die Regelung umfasst auch die verdeckte Videoüberwachung in öffentlich zugänglichen Räumen. Dem steht auch nicht die Regelung des § 6b Abs. 2 BDSG entgegen, wonach die Videoüberwachung an sich erkennbar zu machen ist. Aufgrund der Tatsache, dass es sich bei dieser Regelung nicht um eine Voraussetzung zur Rechtmäßigkeit der Maßnahme, sondern lediglich um eine Ordnungsvorschrift handelt, schließt dies die verdeckte Videoüberwachung aus dem Anwendungsbereich des § 6b BDSG nicht aus und führt nicht zu einem Verbot der verdeckten Videoüberwachung, vgl. dazu *Forst*, RDV 2009, S. 204–211 (209).

Nach den von der Rechtsprechung entwickelten Grundsätzen zur Videoüberwachung ist eine offene Videoüberwachung ebenso zulässig wie die heimliche Videoüberwachung von öffentlich nicht zugänglichen Bereichen.[817] Es kommt dabei für die Rechtmäßigkeit der offenen Videoüberwachung auf die Durchführung einer Prüfung der Verhältnismäßigkeit an. Der Grundsatz der Verhältnismäßigkeit verlangt danach, dass die von den Betriebsparteien bzw. der Einigungsstelle getroffene Regelung geeignet, erforderlich und unter Berücksichtigung der gewährleisteten Freiheitsrechte angemessen ist, um den erstrebten Zweck zu erreichen. Die Angemessenheit von Videoüberwachungsmaßnahmen beurteilt sich maßgeblich nach deren Eingriffsintensität, welche unter anderem von der Anzahl der beobachteten Personen, der Dauer der Überwachung sowie davon abhängig ist, ob die Betroffenen einen zurechenbaren Anlass für ihre Beobachtung gesetzt haben.[818] Insgesamt ist in Bezug auf die Videoüberwachung nach der Rechtsprechung des Bundesarbeitsgerichts im nicht-öffentlichen Bereich zur Beurteilung der Zulässigkeit einer solchen Videoüberwachung auf den Grundsatz der Verhältnismäßigkeit zurückzugreifen.

Für den Fall der Leistungskontrolle wird nach Abwägung der widerstreitenden Interessen von Arbeitgeber und Arbeitnehmer in den meisten Fällen davon auszugehen sein, dass dazu weitere Mittel zur Verfügung stehen, die sich als milderes Mittel darstellen mit der Folge, dass insoweit eine Videoüberwachung im Arbeitsverhältnis nicht rechtmäßig sein wird. Auch im Hinblick auf den Nachweis von strafbaren Handlungen durch Arbeitnehmer wird sich im Einzelfall beispielsweise eine Torkontrolle als milderes Mittel darstellen, um einen Diebstahl durch den Arbeitnehmer nachweisen zu können.[819]

b) Praktischer Anwendungsfall: Einsatz-, Leistungs- und Verhaltenskontrolle

Als praktischer Anwendungsfall kann an dieser Stelle die Leistungs- und Verhaltenskontrolle im Zusammenhang mit der sich fortentwickelnden Technik vernetzter Fahrzeuge relevant werden.

---

817 Vgl. zur offenen Videoüberwachung: Bundesarbeitsgericht, Beschluss vom 26.08.2008, Aktenzeichen 1 ABR 16/07, NZA 2008, S. 1187-1194 sowie Bundesarbeitsgericht, Beschluss vom 29.06.2004, Aktenzeichen 1 ABR 21/03, NZA 2004, S. 1278-1284; vgl. zur verdeckten Videoüberwachung: Bundesarbeitsgericht, Urteil vom 21.06.2012, Aktenzeichen 2 AZR 153/11, NJW 2012, S. 3594-3598; Bundesarbeitsgericht, Urteil vom 27.03.2003, Aktenzeichen 2 AZR 51/02, NZA 2003, S. 1193-1196.

818 Bundesarbeitsgericht, Beschluss vom 26.08.2008, Aktenzeichen 1 ABR 16/07, NZA 2008, S. 1187-1194.

819 So z.B. Bundesarbeitsgericht, Vorlagebeschluss vom 09.07.2013, Aktenzeichen 1 ABR 2/13 (A), NZA 2013, S. 1433-1438.

(i) Szenarien

Es ist an dieser Stelle zu differenzieren zwischen der Einsatzsteuerung einerseits und der Leistungs- und Verhaltenssteuerung andererseits.

Im Bereich des Flottenmanagements besteht ein besonderes Interesse an der Einsatzkontrolle und daran, die Flotte hinsichtlich des Kosten- und Zeitfaktors sinnvoll einzusetzen und zu steuern. Der Schwerpunkt im Rahmen der Einsatzsteuerung und Einsatzkontrolle liegt dabei darauf, die Flotte den Einsätzen entsprechend kurzfristig steuern und so auf aktuelle Gegebenheiten effektiv und schnell reagieren zu können.[820] Die Einsatzkontrolle dient vorwiegend der Routenplanung. So richten Unternehmen bereits ihre Produktangebote im Bereich Software-Lösungen nach diesen Gegebenheiten aus. Beispielhaft sei hierbei auf das Angebot *„MES – Mobile Einsatzsteuerung für die Außendienst-Tourenplanung"*[821] hingewiesen, welches über eine intelligente Plattform zur Anbindung und Steuerung mobiler Mitarbeiter und zur Optimierung der Abläufe dienen soll. Laut Werbeslogan soll die Software das Mobiltelefon oder den PDA zur *„unternehmerischen Allzweckwaffe"* machen. Es werden unter anderen Zeiterfassung und Mitarbeiter-Ortung im Einsatzkontext oder per GPS angeboten. Insoweit besteht bereits ein Markt, der in Bezug auf Einsatzsteuerung eine breite Produktpalette zu bieten hat, in welchem auch die Nachverfolgung der Arbeitnehmer bewusst vom Angebot umfasst ist.[822] Solche Systeme bieten Arbeitgebern und Flottenbetreibern die Möglichkeit, insbesondere anhand der GPS-Daten des Kraftfahrzeugs, des Auflegers, von Anhängern und Containern die mobilen Arbeitnehmer zu steuern. Dies dient wiederum vorwiegend der Kostenreduktion. Die Mitarbeiter können kurzfristig so eingesetzt werden, dass unnötige Umwege auf der Fahrtroute vermieden und dadurch sowohl Personal- als auch Betriebsmittelressourcen geschont werden.

Dadurch ist ebenfalls die Nachverfolgung gestohlener Kraftfahrzeuge oder abhanden gekommener Fracht möglich.

Zusätzlich kann eine Abgrenzung von dienstlicher und privater Nutzung des überlassenen Kraftfahrzeugs vorgenommen werden. Die zurückzulegenden Strecken werden dem

---

820 Vgl. unter *Kapitel 3, Teil 7, III.2.*.

821 Vgl. dazu insgesamt http://www.bmes.de/mes.php.

822 Es finden sich entsprechende Lösungen auch unter den Stichworten „*Flottenmanagement*" oder „*Navigationslösungen für Geschäftskunden*" bei zahlreichen Anbietern entsprechender Hard- und Software, vgl. *Wedde* in DKWW: Bundesdatenschutzgesetz, [4]2014, § 32, Rn. 104.

mobilen Arbeitnehmer im Bereich des Flottenmanagements vorgegeben. Ein nachträglicher Abgleich von vordefinierter und tatsächlich gefahrener Strecke durch den Arbeitgeber könnte sodann ergeben, dass vom Arbeitnehmer nicht die vorgegebene Strecke gefahren und somit der Einsatz nicht optimal ausgeführt wurde.

Aber auch die Verhaltens- und Leistungskontrolle und die Steuerung derselben spielen eine gewichtige Rolle. Die Vernetzung des Kraftfahrzeugs bietet unter anderem durch die Anwendung von Big Data die Möglichkeit, alle aus dem Kraftfahrzeug zu generierenden Daten miteinander zu verknüpfen und auf diese Weise die Arbeitnehmer und deren Leistung zu überwachen, was allerdings bei der Anwendung technischer Einrichtungen dazu führt, dass ein Mitbestimmungsrecht des Betriebsrates zu beachten ist.[823]

Während durch Ortung der Mitarbeiter die Möglichkeit zur Einsatzsteuerung geschaffen wird, kann der Zweck der Ortung aber auch darin liegen, z.B. die Einhaltung der Arbeitszeit durch die Arbeitnehmer zu kontrollieren.[824] Die GPS-Daten liefern Informationen darüber, wo sich ein Arbeitnehmer mit dem Dienstfahrzeug zu welcher Zeit aufhält. Die Streckendaten geben aber auch Auskunft darüber, zu welcher Zeit das Kraftfahrzeug bewegt wurde und entlang welcher Strecke. Aber auch durch Übertragung von Standortdaten kann eine Leistungs- und Verhaltenskontrolle stattfinden, wenn die dabei übertragenen Daten es ermöglichen, ein Bewegungsprofil des Arbeitnehmers als Fahrer zu generieren.[825] Dadurch könnte überwacht werden, wo sich der Arbeitnehmer wie lange aufhält und ob er beispielsweise den direkten Weg zum nächsten Arbeitsort wählt oder aber Umwege fährt und sich anhand der Daten herausfinden lässt, dass der Arbeitnehmer womöglich auf dem gewählten Umweg noch private Angelegenheiten erledigt. Dies dient sodann der Leistungs- und Verhaltenskontrolle. Auch ist anhand dessen nachvollziehbar, ob die vom Arbeitnehmer gemachten Angaben über den Umfang von Privatfahrten korrekt sind.

An der Nachvollziehbarkeit dessen hat der Arbeitgeber insbesondere auch im Hinblick auf versicherungsrechtliche Gründe und auf einen versicherungskonformen Umgang mit dem Dienstfahrzeug ein hohes Interesse.

Zuletzt spielen aber auch hier die Aspekte der Ressourcenschonung und Kostenersparnis eine Rolle. Um Kraftstoff zu sparen und die Kosten für Reparaturen und Verschleiß-

---

823 Vgl. unter *Kapitel 3, Teil 7, II.*.
824 Vgl. unter *Kapitel 3, Teil 7, III.2.*.
825 Vgl. unter *Kapitel 3, Teil 7, III.1.*.

teile gering zu halten, könnte der Arbeitgeber ein Interesse daran haben, ein Bonussystem einzuführen, mit welchem er den Arbeitnehmer zu einem schonenderen Fahrverhalten motiviert, um dies anhand der übermittelten Daten kontrollieren zu können. All diese vorgenannten Punkte werden mit der weiteren Vernetzung von Kraftfahrzeugen weiter an Relevanz gewinnen.

(ii) Rechtliche Würdigung

Für die rechtliche Beurteilung von Einsatz- und Verhaltenssteuerung kommt es vorwiegend auf die Regelung des § 28 Abs. 1 BDSG an.

Die rechtliche Zulässigkeit einer Einsatz- und Verhaltenssteuerung kann sich allerdings nur ausnahmsweise aus der Vorschrift des § 28 Abs. 1 BDSG ergeben. In Betracht kommt zunächst der Erlaubnistatbestand des § 28 Abs. 1 Satz 1 Nr. 1 BDSG, wonach personenbezogene Daten zulässigerweise für die Erfüllung eigener Geschäftszwecke verwendet oder genutzt werden dürfen, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

Dabei ist zu beachten, dass das geschäftliche Interesse nicht gerade in der Datenverwendung selbst liegt, sondern dass der eigentliche Hauptzweck in der Abwicklung eines rechtsgeschäftlichen Schuldverhältnisses liegt.[826] Es muss hier also auf einen Vertragszweck abgestellt werden, welcher die Datenverwendung rechtfertigen könnte. Dies ist insbesondere denkbar im Zusammenhang mit der Erfüllung gesetzlicher Vorgaben bei Geldtransporten.[827] Hierbei ist die Sicherheit des Lebens des Betroffenen sowie von äußerst wertvollem Unternehmenseigentum als Vertragszweck anzuerkennen und eine Datenverwendung zu diesem Zweck als erforderlich anzusehen. Wird ein Geldtransporter zu vorgenannten Zwecken mittels GPS geortet, so kann dies über die Norm des § 28 Abs. 1 Satz 1 Nr. 1 BDSG gerechtfertigt werden.

Die datenschutzrechtliche Zulässigkeit kann sich im Einzelfall auch aus dem Erlaubnistatbestand des § 28 Abs. 1 Satz 1 Nr. 2 BDSG ergeben. Danach dürfen personenbezogene Daten zulässigerweise für die Erfüllung eigener Geschäftszwecke verwendet oder genutzt werden, soweit es zur Wahrung berechtigter Interessen der verantwortlichen

826 Vgl. unter *Kapitel 3, Teil 3, I.1.a)(i).*
827 Vgl. *Kremer*, RDV 2014, S. 240–252 (251).

Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Verarbeitung oder Nutzung überwiegt.

Maßgeblich ist insoweit eine Interessenabwägung zwischen den berechtigten Interessen der verantwortlichen Stelle und den schutzwürdigen Interessen des Betroffenen.[828] Standortdaten können aufgrund dieses Erlaubnistatbestands beispielsweise verwendet werden für die Notfallplanung im Facility Management sowie die Ressourcen- und Routenplanung im Logistik-Bereich.[829] Beispielsweise sollen Speditionen den Einsatz des Fuhrparks mithilfe von Ortungssystemen koordinieren dürfen.[830] Hierbei ist ausgehend von dem mit der jeweiligen Maßnahme verfolgten Zweck davon auszugehen, dass die berechtigten Interessen der verantwortlichen Stelle überwiegen. Für die Ressourcenschonung und die effiziente Routenplanung im Bereich des Logistikmanagements ist es notwendig, dass Flottenbetreiber Zugriff auf die Standorte der einzelnen Flottenfahrzeuge haben, um diese dann entsprechend kurzfristig einsetzen und etwaige Änderungen der Route bekanntgeben zu können.

Das berechtigte Interesse des Flottenbetreibers liegt darin, insbesondere für kurzfristige Einsätze auf denjenigen Mitarbeiter zurückgreifen zu können, für den dieser Einsatz auf der Route liegt bzw. den kürzesten Umweg bedeutet. Dadurch können im Bereich des Flottenmanagements Zeit, Geld und Betriebsmittel gespart werden. Dieses Interesse überwiegt das Interesse des betroffenen Arbeitnehmers daran, nicht preisgeben zu wollen, wo er sich während der Arbeitszeit gerade aufhält und welche Strecken von ihm zurückgelegt werden.

Allerdings ist in diesen Fällen zu beachten, dass dabei eine strenge Zweckbindung anzulegen ist. Zudem müssen diese Daten nach Zweckerledigung unverzüglich gelöscht werden, dürfen nicht mit anderen personenbezogenen Daten zusammengeführt oder etwa im Privatbereich erhoben werden, sofern die Systeme nach Beendigung der Arbeitszeit nicht deaktiviert werden.[831] Es ist hier jedoch sicherzustellen, dass solche Systeme ausschließlich während der Arbeitszeit aktiviert sind. Denn der Zweck der Einsatzplanung hat sich lediglich auf die Arbeitszeit zu beziehen, um innerhalb derer die

828 Vgl. unter *Kapitel 3, Teil 3, I.1.b)*.
829 Vgl. *Kremer*, RDV 2014, S. 240–252 (251).
830 Vgl. Eckpunkte-Papier des Bundesministeriums des Inneren zum Beschäftigtendatenschutz vom 31.03.2010, S. 4, http://www.bmi.bund.de/cae/servlet/contentblob/941830/publicationFile/60604/eckpunkte_an_datenschutz.pdf.
831 So *Kremer*, RDV 2014, S. 240–252 (251).

Betriebsmittel schonend und sparsam einzusetzen. In der Freizeit kann dies jedoch nicht mehr durch die Interessen der verantwortlichen Stelle gerechtfertigt werden.

Sofern die vorgenannten Voraussetzungen nicht vorliegen und insbesondere durch die Verwendung der Standortdaten die Zweckbindung nicht eingehalten wird, kann die Zulässigkeit der Datenverwendung nur durch die Einholung einer wirksamen Einwilligung des Betroffenen erreicht werden. Allerdings besteht auch an dieser Stelle erneut die Problematik der Freiwilligkeit einer vom Arbeitnehmer im Rahmen des Arbeitsverhältnisses erteilten Einwilligung.[832]

Zuletzt sei in diesem Zusammenhang noch auf ein etwaig bestehendes Mitbestimmungsrecht des Betriebsrates nach § 87 Abs. 1 Nr. 6 BetrVG hingewiesen. Durch Maßnahmen, insbesondere der Ortung muss von einer tatbestandlichen Überwachung der Leistung und des Verhaltens des Arbeitnehmers durch technische Einrichtungen ausgegangen werden.[833] GPS-Systeme zeichnen gerade auch Informationen über das Fahrverhalten auf, sodass deren Einsatz deshalb nach der Rechtsprechung des Bundesarbeitsgerichts als mitbestimmungspflichtige Maßnahme einzustufen sei.[834] Ortungsmaßnahmen sind dazu bestimmt, die Leistung des Arbeitnehmers dadurch zu überwachen, dass durch die daraus generierten Daten eine Überprüfung stattfinden kann, ob sich der Arbeitnehmer entsprechend der vom Arbeitgeber gemachten Vorgaben verhält.

c) Praktischer Anwendungsfall: Verfolgung und Ahndung von Ordnungswidrigkeiten und Straftaten

Eine weitere praktisch relevante Fallgruppe ist in der Verfolgung und Ahndung von Ordnungswidrigkeiten und Straftaten zu sehen, die durch das Kraftfahrzeug oder mithilfe dessen begangen wurden und bei denen der Fahrer durch die Daten aus dem Kraftfahrzeug überführt werden könnte.

---

832 Die Problematik wurde bereits im Rahmen der Ortung von Arbeitnehmern und im Zusammenhang mit einem bestehenden Mitbestimmungsrecht des Betriebsrats angeführt, vgl. unter Kapitel 3, Teil 7, III.2.; vgl. zur Problematik der Freiwilligkeit einer im Arbeitsverhältnis erteilten Einwilligung insgesamt unter *Kapitel 3, Teil 3, II.3.b)*.

833 Vgl. unter *Kapitel 3, Teil 7, II.* sowie unter *Kapitel 3, Teil 7, III.2.*.

834 Bundesarbeitsgericht, Beschluss vom 10.12.2013, Aktenzeichen 1 ABR 43/12, DuD 2014, S. 633-634.

(i) Szenarien

Das klassische Szenario, das sich in diesem Teilbereich abspielen könnte, ist eine Geschwindigkeitsüberschreitung durch den Fahrer. Nach dem neuen Bußgeldkatalog müsste der Fahrer bei einer Geschwindigkeitsüberschreitung von mindestens 41 km/h Außerorts mit einer Geldbuße in Höhe von 160,- Euro, zwei Punkten im Verkehrszentralregister und einem Monat Fahrverbot rechnen.[835]

Dieser Verstoß ließe sich anhand der Verknüpfung der Geschwindigkeitsdaten aus dem Kraftfahrzeug mit den Verkehrsdaten leicht nachweisen. Über die Verkehrsdaten würden die Behörden Kenntnis darüber erlangen, welche Strecke gefahren und wie hoch eine etwaige Begrenzung der Höchstgeschwindigkeit an dieser Stelle festgelegt wurde. Werden diese Daten danach mit den persönlichen Geschwindigkeitsdaten des Fahrers verknüpft, kann ohne weiteres ein Fehlverhalten nachgewiesen werden.

Durch die Vernetzung des Kraftfahrzeugs kann dieses Szenario auch noch erweitert werden. Gerade durch die Möglichkeiten, die sich durch Telematik und Verbindung des Kraftfahrzeugs mit mobilen Endgeräten ergeben, könnte es möglich sein, den Fahrer anhand verschiedener Daten individuell bestimmen zu können. Dies könnte über die beim Versicherer hinterlegten Fahrerdaten, auf den Fahrer gerichtete Kameras[836] oder ein verknüpftes persönliches Smart Device[837] des Fahrers ermöglicht werden. Sofern aufgrund dessen ein Fahrer individuell bestimmt werden kann und auch weitere personenbezogene Daten von ihm vorliegen, könnte ein Bußgeldbescheid zukünftig automatisch nach der Anschrift des Betroffenen versendet und dem Fahrer gleichzeitig eine digitale Ausführung desselben über das Mobilfunknetz auf sein Smart Device und somit in das Kraftfahrzeug geschickt werden.

Die Abwicklung des Ordnungswidrigkeitsverfahrens könnte sodann über die im Kraftfahrzeug vorhandenen Schnittstellen[838] erfolgen. Über den Bordcomputer könnte der Fahrer ohne großen Zeitverlust und mit wenig Aufwand die Zahlung der Geldbuße anweisen. Es könnte zukünftig möglich sein, die Abrechnung der Zahlung als Mehrwertdienst über die im Kraftfahrzeug fest verbaute SIM-Karte oder über Online-Banking die

---

835 Vgl. http://www.bussgeld-info.de/bussgeldkatalog-geschwindigkeit/.
836 Vgl. unter *Kapitel 2, Teil 2, I.2.b).*
837 Vgl. unter *Kapitel 2, Teil 4, II.1.*.
838 Vgl. unter *Kapitel 2, Teil 3, I.*.

Überweisung sofort vorzunehmen. All dies sind Facetten der sich entwickelnden Car to X-Kommunikation.

Ebenso ist es denkbar, dass eine Straftat seitens des Fahrers begangen wird, bei der das Kraftfahrzeug selbst eine Rolle spielt. Dies kann einerseits in der Gestalt relevant werden, dass ein Unfall verursacht wird und der Fahrer anschließend mit seinem Kraftfahrzeug Unfallflucht begeht. Andererseits könnte das Kraftfahrzeug aber auch beispielsweise im Rahmen eines Bankraubes als Fluchtfahrzeug genutzt werden. Letzteres unter der Prämisse, dass das Fahrzeug zunächst nicht von Zeugen identifiziert würde.

Zur unmittelbaren Überführung des Straftäters könnte sich die Strafverfolgungsbehörde zunächst der Versicherer bedienen und bei diesen unter Angabe des Tatorts und der Tatzeit die zum tatrelevanten Zeitpunkt am Tatort befindlichen Kraftfahrzeuge abfragen. Aber die Vernetzung der Kraftfahrzeuge mit der umliegenden Infrastruktur würde es ebenfalls ermöglichen, dass Strafverfolgungsbehörden die FIN eines Kraftfahrzeugs über in der näheren Umgebung aufgestellte intelligente Verkehrssysteme, wie z.B. Ampelanlagen oder Mautbrücken, selbst ermitteln und das Fahrzeug identifizieren. Nachdem sodann das Tatfahrzeug ermittelt worden ist, könnte die die Verfolgung aufnehmende Streifenwagenbesatzung auf das technisch in der Entwicklung begriffene Instrument der Fernabschaltung von Kraftfahrzeugen zurückgreifen und dadurch das Kraftfahrzeug ohne Zutun des Fahrers zum Stillstand bringen. Zuletzt könnte im Zusammenhang mit der Strafverfolgung ein etwaiges vom Fahrer im Strafprozess angegebenes Alibi unter Zuhilfenahme der Daten auf seine Richtigkeit überprüft werden. Anhand der Aussage des Fahrers können u.a. die Streckendaten des Navigationsgeräts darauf überprüft werden, ob der Fahrer sich nicht doch zum Tatzeitpunkt am Tatort aufgehalten haben könnte. Dies zeigt insgesamt, welche technischen Möglichkeiten den Strafverfolgungsbehörden zur Verfügung stehen. Dabei werden sämtlich die durch das Kraftfahrzeug generierten Daten gegen den Fahrer verwendet.

(ii) Rechtliche Würdigung

Es stellt sich jedoch die Fragen, ob all die vorgenannten Szenarien in datenschutzrechtlicher Hinsicht zulässig sind.

Als Erlaubnistatbestände für die vorgenannten einzelnen Szenarien kommen hier im Sinne des § 4 Abs. 1 BDSG jeweils verschiedene Vorschriften der Strafprozessordnung in Betracht.

Zunächst richtet sich die Zulässigkeit der Sicherstellung und Beschlagnahme von Daten als Beweismittel nach § 94 StPO.[839]

Da eine Sicherstellung nur beim Gewahrsamsinhaber in Betracht kommt[840], können hier verschiedene Akteure in Betracht kommen. Sofern es sich um Daten handelt, auf die der Fahrer oder ein sonstiger Dritter keinen Zugriff hat und lediglich der Hersteller die Herrschaft über diese Daten ausüben kann, ist auch nur der Hersteller als Gewahrsamsinhaber anzusehen, bei dem die Daten sodann zu beschlagnahmen wären. Dies betrifft insbesondere die rein technischen Messdaten. Aber auch Diensteanbieter können als Gewahrsamsinhaber eingestuft werden. Dies gilt, wenn es sich bei den zu beschlagnahmenden oder sicherzustellenden Daten um solche Daten handelt, die beim Diensteanbieter bei der Nutzung des Dienstes durch den Fahrer anfallen. Denkbar sind Informationen über Verbindungsnachweise oder die Nutzung des Dienstes an sich. Der Fahrer kann in diesen Fällen nicht als Gewahrsamsinhaber angesehen werden, selbst wenn ihm Einzelverbindungsnachweise zur Verfügung gestellt werden. Ihm liegen diese Informationen dann zwar vor, Einfluss nehmen kann er darauf jedoch nicht.

Allerdings sind auch Fälle denkbar, in denen der Fahrer selbst als Gewahrsamsinhaber in Betracht kommt. Vor allem hinsichtlich der Daten, die er selbst jeweils in den Bordcomputer eingibt und die er unproblematisch selbst beeinflussen kann, ist dies anzunehmen. Beispielsweise liegen seine Kontakte, die über das Smartphone in das Kraftfahrzeug gelangen, in seiner Sachherrschaft. Gewahrsam über diese Daten liegt hier vor. Insgesamt ist jedoch für jeden Einzelfall zu prüfen, wer als Gewahrsamsinhaber und somit als Zielperson für eine Sicherstellung bzw. Beschlagnahme einzuordnen ist, bei dem letztlich die Sicherstellung bzw. Beschlagnahme seitens der Strafverfolgungsbehörden stattfindet.

Allerdings ist hierbei stets zu beachten, dass nur solche Beweismittel sichergestellt bzw. beschlagnahmt werden dürfen, die für die Untersuchung von Bedeutung sind, d.h. für jede Tätigkeit im Strafverfahren, die der Aufklärung des Tatbestandes oder sonst der

839 Vgl. dazu unter *Kapitel 3, Teil 6, V.*.
840 Vgl. unter *Kapitel 3, Teil 6, V.*.

Vorbereitung des gerichtlichen Verfahrens dient.[841] Es genügt dabei jedoch die nachvollziehbare Erwartung, dass der Gegenstand oder dessen Untersuchung Schlüsse auf entscheidungserhebliche Tatsachen zulässt.[842]

Die Daten aus dem Kraftfahrzeug dürfen insoweit nur dort genutzt werden, wo dies sinnvoll erscheint. Erforderlich ist dabei eine Beziehung des Kraftfahrzeugs zur Tat. Die Tatbegehung muss mit der Benutzung des Kraftfahrzeugs unmittelbar zusammenhängen. Denn nur so können sich entscheidungserhebliche Tatsachen aufklären lassen. Ohne Anhaltspunkte beispielsweise auf eine Flucht mit einem Kraftfahrzeug würde es sich nicht rechtfertigen lassen, sämtliche Kraftfahrzeuge über die Daten aus Intelligenten Verkehrssystemen zu identifizieren.

In Bezug auf eine Sicherstellung oder Beschlagnahme ist jedoch ein etwaig bestehendes Beschlagnahmeverbot gemäß § 97 Abs. 1 Nr. 1 StPO iVm § 52 StPO zu beachten. Danach unterliegen schriftliche Mitteilungen zwischen dem Beschuldigten und zeugnisverweigerungsberechtigten Personen im Sinne von § 52 StPO nicht der Beschlagnahme. Als schriftliche Mitteilungen sind alle Gedankenäußerungen, die ein Absender einem Empfänger zukommen lässt, damit er davon Kenntnis nimmt, umfasst, wie z.B. E-Mails, Mitteilungen durch Zeichnungen oder auf Bild- und Tonträgern. [843] Inhalt und Zweck der Mitteilung sind bei dem zeugnisverweigerungsberechtigten Personenkreis nach § 52 StPO nicht relevant.[844]

Soweit also z.B. E-Mails über die Verbindung des Smartphones mit dem Kraftfahrzeug auch im Kraftfahrzeug empfangen und gelesen werden können, ist davon auszugehen, dass diese als schriftliche Mitteilungen grundsätzlich unter das Beschlagnahmeverbot nach § 97 Abs. 1 Nr. 1 StPO fallen. Umfasst ist davon jedoch nicht sämtlicher E-Mail-Verkehr. Vielmehr gilt das Beschlagnahmeverbot nur in Bezug auf solche E-Mails, die zeugnisverweigerungsrechtlichen Personen nach § 52 StPO zur Kenntnis gelangen und für diese bestimmt sind.

Ein weiterer Aspekt ist in Bezug auf Beschlagnahmen auch der nach § 98 StPO grundsätzlich zu beachtende Richtervorbehalt. Nach § 98 Abs. 1 StPO dürfen Beschlagnahmen nur durch das Gericht angeordnet werden. Nur bei Gefahr im Verzug kann die An-

841 Vgl. *Joecks*: Strafprozessordnung, [4]2015, § 94, Rn. 3.
842 Vgl. *Eschelbach* in Satzger/Schluckebier/Widmaier: StPO, [1]2014, § 94 StPO, Rn. 15.
843 Vgl. *Schmitt* in Meyer-Goßner/Schmitt: Strafprozessordnung, [58]2015, § 97, Rn. 28.
844 Vgl. *Joecks*: Strafprozessordnung, [4]2015, § 97, Rn. 10.

ordnung der Beschlagnahme auch durch die Staatsanwaltschaft oder ihr Ermittlungspersonen erfolgen. Es drängt sich dabei die Frage auf, ob bei der Beschlagnahme von Daten aus dem Kraftfahrzeug tatsächlich Konstellationen vorliegen können, die die Annahme von Gefahr in Verzug rechtfertigen. Denn der Begriff *„Gefahr in Verzug"* ist wegen des Ausnahmecharakters der nichtrichterlichen Anordnung und der grundrechtssichernden Schutzfunktion des Richtervorbehalts eng auszulegen.[845] Danach liegt Gefahr in Verzug vor, wenn aufgrund bestimmter Tatsachen anzunehmen ist, dass das Beweismittel verloren geht und dadurch der meist maßgebliche Beweissicherungszweck der Maßnahme verfehlt würde, sofern vor dem Beschlagnahmezugriff auf den Beweisgegenstand zuerst eine richterliche Anordnung eingeholt wird.[846]

Dies kann für nur kurzzeitig im Kraftfahrzeug oder auf einem Datenträger gespeicherte Daten Relevanz besitzen. Die sog. flüchtigen Daten werden direkt nach ihrer Erhebung genutzt und unmittelbar danach wieder gelöscht oder überschrieben.[847] Auf welche Daten aus dem Kraftfahrzeug dies zutrifft, kann mangels Informationen seitens der Hersteller nicht abschließend beurteilt werden. Jedoch ist davon auszugehen, dass es in jedem Fall auch nur kurzzeitig gespeicherte Daten gibt. Eine Eilkompetenz der Staatsanwaltschaft bzw. ihrer Ermittlungspersonen kann tatsächlich nur dann angenommen werden, wenn das Beweismittel dadurch insgesamt verloren ginge und dadurch der Beweissicherungszweck vereitelte würde.

Mit Rücksicht auf die Vielzahl der im Kraftfahrzeug anfallenden Daten ist hier davon auszugehen, dass Gefahr im Verzug nur angenommen werden kann, wenn sich aus keinen der sonst anfallenden Daten dieselben Informationen gewinnen lassen. Auch im Hinblick auf die gebotene enge Auslegung des Merkmals ist grundsätzlich ein Richtervorbehalt anzunehmen, solange auch noch andere Daten zur Verfügung stehen, die den gleichen oder einen ähnlichen Informationsgehalt aufweisen und somit zu demselben Ermittlungsergebnis führen würden. Dies darf nicht dadurch umgangen werden, dass auf dieselben Daten zurückgegriffen wird, die im Gegensatz dazu jedoch nur kurzfristig gespeichert werden, nur um dadurch den Richtervorbehalt auszuhebeln.

Als Erlaubnisnachtatbestand nach § 4 Abs. 1 BDSG könnte hier auch die Vorschrift des § 100a StPO in Betracht kommen. Beim Verdacht schwerer Straftaten gegen den Fahrer

---

845 Vgl. *Hauschild* in Kudlich: MüKo StPO, Band 1, 2013, § 98, Rn. 8.
846 Vgl. nur *Eschelbach* in Satzger/Schluckebier/Widmaier: StPO, [1]2014, § 98 StPO, Rn. 11.
847 Vgl. unter *Kapitel 2, Teil 2*.

eines Kraftfahrzeugs könnte die vom Kraftfahrzeug ausgehende Telekommunikation überwacht werden. Gemäß § 100a StPO darf die Telekommunikation auch ohne Wissen des Betroffenen überwacht werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in § 100a Abs. 2 StPO bezeichnete schwere Straftat begangen hat, die Tat auch im Einzelfall schwer wiegt und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtlos wäre. Sofern also im Einzelfall eine nach § 100a Abs. 2 StPO näher bezeichnete schwere Straftat vorliegt, kommt eine Überwachung der Telekommunikation bei Vorliegen der vorgenannten Voraussetzungen in Betracht.

Sofern das Smartphone über eine Drahtlosverbindung mit dem Kraftfahrzeug verbunden ist und dabei die Gespräche über die Lautsprecher des Kraftfahrzeugs übertragen werden, ist trotz der Verbindung mit dem Kraftfahrzeug weiterhin von *„Telekommunikation“* im Sinne des § 100a StPO auszugehen. Es wurde bereits darauf hingewiesen, dass die Differenzierung zwischen Telekommunikation und Telemedien aufgrund der technischen Ausgestaltung mitunter schwierig sein kann.[848] Deshalb ist auch hier im Einzelfall genau zu prüfen, ob bei den einzelnen Anwendungen tatsächlich Telekommunikation in diesem Sinne vorliegt. Nur dann kommt auch die Anwendung des § 100a StPO als Erlaubnistatbestand gemäß § 4 Abs. 1 BDSG in Betracht.

Daneben verdient ebenso die Vorschrift des § 100f Abs. 1 StPO hier Beachtung. Auch ohne das Wissen des Betroffenen darf danach außerhalb von Wohnungen das nichtöffentlich gesprochene Wort mit technischen Mitteln abgehört und aufgezeichnet werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in § 100a Abs. 2 StPO bezeichnete, auch im Einzelfall schwerwiegende Straftat begangen hat und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts eines Beschuldigten auf andere Weise aussichtlos oder wesentlich erschwert wäre. Die Maßnahme darf sogar dann durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.[849] Grundsätzlich ist also auch eine akustische Überwachung von Kraftfahrzeugen zulässig, sofern tatsächlich vom Vorliegen einer schweren Straftat auszugehen ist.

---

848 Vgl. unter *Kapitel 3, Teil 3, III.*

849 Vgl. § 100f Abs. 3 StPO.

Etwas anderes gilt nach der Rechtsprechung des Bundesgerichtshofs in Bezug auf die Verwertbarkeit der daraus erlangten Informationen. Für den Fall eines in einem Kraftfahrzeug mittels akustischer Überwachung aufgezeichneten Selbstgespräches eines sich unbeobachtet fühlenden Beschuldigten seien die daraus gewonnen Informationen im Strafverfahren – auch gegen Mitbeschuldigte – unverwertbar, da dies dem durch Art. 2 Abs. 1 iVm Art. 1 Ab. S 1 GG absolut geschützten Kernbereich der Persönlichkeit zuzurechnen sei.[850] Es ist in solchen Konstellationen mithin danach zu differenzieren, ob tatsächlich ein nach der Rechtsprechung geschütztes Selbstgespräch vorliegt, bei dem die Informationen zwar erhoben, aber gerade nicht verwertet werden dürfen, oder ob es sich vielmehr um ein allgemeines Gespräch mit Insassen oder Dritten handelt.

Zuletzt könnte als Erlaubnistatbestand auch die Vorschrift des § 100i StPO herangezogen werden. Begründen danach bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 StPO bezeichnete Straftat, begangen hat, dürfen durch technische Mittel die Gerätenummer eines Mobilfunkendgerätes und die Kartennummer der darin verwendeten Karten sowie der Standort eines Mobilfunkendgerätes ermittelt werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist. Die Vorschrift zielt auf die Anwendung sog. „IMSI-Catcher“[851] ab. Als fraglich erweist sich im vorliegenden Kontext jedoch, ob es sich bei dem Kraftfahrzeug, in welches eine SIM fest verbaut ist, auch um ein Mobilfunkendgerät handelt. Andernfalls wäre bereits der Anwendungsbereich der Vorschrift nicht eröffnet. Allerdings ist hier davon auszugehen, dass kein wesentlicher Unterschied zwischen der Verbindung des Mobiltelefons mit dem Kraftfahrzeug mittels Drahtlosverbindung und dem festen Einbau einer SIM Karte im Kraftfahrzeug besteht.[852] Gleiches muss auch in diesem Zusammenhang gelten. Denn die Gerätenummer bleibt in beiden Fällen nachvollziehbar.

Insgesamt existieren somit einige Erlaubnistatbestände aus den Vorschriften der Strafprozessordnung, die eine Datenverwendung vor dem Hintergrund erlauben, die Daten

---

850 Bundesgerichtshof, Urteil vom 22.12.2011, Aktenzeichen 2 StR 509/10, NJW 2012, S. 945-947 (Leitsatz).

851 Über die Kennung IMSI („*International Mobile Subscriber Identity*“, deutsch Kartennummer) können Positions- und Standortmeldungen von aktiv geschalteten Mobilfunkanschlüssen ermittelt werden, vgl. Schmitt in Meyer-Goßner/Schmitt: Strafprozessordnung, [58]2015, § 100i, Rn. 1.

852 Vgl. unter *Kapitel 3, Teil 7, III.1.*.

im Rahmen eines Ordnungswidrigkeiten- oder Strafverfahrens gegen den Betroffenen einzusetzen. Regelmäßig setzt dies jedoch das Vorliegen einer schweren Straftat voraus.

6. Zusammenfassung zu den praktischen Anwendungsfällen

Zusammenfassend lässt sich festhalten, dass die Masse der denkbaren Verwendungsmöglichkeiten für Daten aus dem Kraftfahrzeug in der Praxis weitreichende Auswirkungen für den Betroffenen mit sich bringen kann. In allen vorgenannten Fällen würde eine Datenverwendung jeweils zum Nachteil des Betroffenen stattfinden, unabhängig davon, ob es dabei um die Geltendmachung von Regressansprüchen oder um die Verfolgung von Straftaten und Ordnungswidrigkeiten geht. Der Betroffene wird hier seine Einwilligung zur Datenverwendung nicht erteilen. Die gesetzlichen Erlaubnistatbestände decken die praktischen Fallgestaltungen zwar ab, dies jedoch nur, wenn diese in engem Zusammenhang mit dem Beschäftigungsverhältnis steht. Letztlich kann zum jetzigen Zeitpunkt noch nicht abgesehen werden, welche Dimensionen die technische Entwicklung noch erreichen wird. Somit sind die genannten Fallgruppen beliebig erweiterbar. Es hat hier eine Einzelfallbetrachtung zu erfolgen.

7. Umfang des Mitbestimmungsrechts

Vom Umfang her erstreckt sich das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG sowohl auf die Einführung als auch auf die Anwendung von technischen Einrichtungen. Unter der Einführung von technischen Einrichtungen ist dabei die Entscheidung in Bezug auf das *„Ob“* und die Frage, für welchen Zeitraum, an welchem Ort, mit welcher Zweckbestimmung und Wirkungsweise zu verstehen, während die Anwendung der technischen Einrichtung auf ihre allgemeine Handhabung sowie auf die Art und Weise abstellt, wie sie tatsächlich zur Kontrolle verwendet wird.[853] Der Terminologie nach betrifft die *„Einführung“* das *„Ob“* und die *„Anwendung“* das *„Wie“*.[854]

Sofern eine mitbestimmungspflichtige Maßnahme allerdings letztlich ohne die notwendige Zustimmung des Betriebsrats durchgeführt wird, besteht für den Betriebsrat die Möglichkeit, gegen die Maßnahme im Wege der einstweiligen Verfügung vorzugehen.

---

853 Vgl. *Klebe* in DKKW: BetrVG, [14]2014, § 87, Rn. 170, 173

854 Vgl. *Richardi* in Richardi: Betriebsverfassungsgesetz, [14]2014, § 87, Rn. 513.

III. Weitere mitbestimmungspflichtige Maßnahmen

Im Folgenden sollen an dieser Stelle einige weitere in der Praxis mögliche Maßnahmen von Seiten des Arbeitgebers in Bezug auf die Datenverwendung aus vernetzten Fahrzeugen dargestellt werden, die insoweit ebenfalls einem Mitbestimmungsrecht unterliegen. Dies betrifft die Übertragung von Standortdaten, die Ortung externer Mitarbeiter sowie den Einsatz von Fahrtenschreibern.

1. Übertragung von Standortdaten

Die Übertragung von Standortdaten spielt im Zusammenhang mit der Datenverwendung aus vernetzten Fahrzeugen insbesondere im Hinblick auf die Nutzung von Mobiltelefonen im Kraftfahrzeug eine Rolle. Dabei dreht es sich oftmals um mit in das Kraftfahrzeug verbrachte Mobiltelefone und Smartphones, die jedoch nicht fest mit dem Kraftfahrzeug verbunden sind. Hierbei richtet sich die Erlaubnis zur Datenverwendung nach der spezialgesetzlichen Vorschrift des § 98 TKG.

a) Übertragungsweg SIM-Karte

Nicht selten werden jedoch im Arbeitsverhältnis den Arbeitnehmern Dienstfahrzeuge überlassen, in denen bereits SIM-Karten verbaut sind.

Es stellt sich dabei die Frage, ob auch für den Fall der bereits im Kraftfahrzeug verbauten SIM-Karten die Regelung des § 98 TKG Anwendung findet.

Auch und gerade wenn bereits ein Einbau der SIM-Karte im Fahrzeug erfolgt ist, muss von einer Überwachung der Telekommunikation des Arbeitnehmers ausgegangen werden. Es herrscht eine vergleichbare Gefährdungslage wie im Fall der Verbringung des Mobiltelefons in das Kraftfahrzeug durch den Arbeitnehmer. Auch die technische Ausgestaltung ist nahezu identisch. In beiden Fällen ist es zudem möglich, den Arbeitnehmer durch die Kontrolle der Telekommunikation zu überwachen. Es kann in beiden Fällen dadurch der Standort ermittelt werden. Diese Informationen können sodann zur unzulässigen Leistungskontrolle genutzt werden. Die Gefahr besteht in beiden Fällen. Insoweit sind hier eine identische technische Ausgestaltung sowie eine vergleichbare Gefährdungslage und ein entsprechendes Risiko gegeben.

Die nunmehr folgenden Grundsätze sind somit auch auf die Situation übertragbar, in denen eine feste Verbindung zwischen Kraftfahrzeug und Telekommunikation durch

Einbau von SIM-Karten stattfindet. Es ist demnach die Ortung unmittelbar über die fest verbaute SIM-Karte im Fahrzeug ebenso als Anwendungsfall einzuordnen wie der Fall, dass der Diensteanbieter mittels eines mit dem Kraftfahrzeug verbundenen Mobiltelefons den Standort des Fahrzeugs ermittelt und diese Standortdaten sodann von ihm selbst oder einem Anbieter von Diensten mit Zusatznutzen verwendet werden.[855] In beiden Fällen sind eine Ortung des Arbeitnehmers und damit auch eine Überwachung seiner Leistung möglich.

b) Erlaubnistatbestand des § 98 TKG

In der Verwendung von Standortdaten ist zunächst eine Überwachung im Sinne des § 87 Abs. 1 Nr. 6 BetrVG zu sehen, die ein Mitbestimmungsrecht des Betriebsrates auslöst. Werden diese Standortdaten sodann im weiteren Verlauf nach der Erhebung auch übertragen, birgt dies wiederum Gefahren im Hinblick auf das Persönlichkeitsrecht der Betroffenen. Die Schutzbedürftigkeit von Standortdaten ergibt sich zudem in besonderem Maße daraus, dass durch die Verwendung derselben die Möglichkeit eröffnet wird, umfassende Bewegungsprofile der Betroffenen zu erstellen.

Insoweit ist für diese Fälle die Vorschrift des § 98 TKG zu beachten. Dort wird die Bereitstellung von Diensten mit Zusatznutzen unter Verwendung von Standortdiensten geregelt.[856] Nach § 98 Abs. 1 Satz 1 TKG dürfen Standortdaten, die in Bezug auf die Nutzer von öffentlichen Telekommunikationsnetzen oder –diensten für die Öffentlichkeit verwendet werden, nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Teilnehmer seine Einwilligung erteilt hat. Mitbenutzer sind von dem Teilnehmer über eine erteilte Einwilligung nach § 98 Abs. 1 Satz 2 TKG zu unterrichten.

Als Teilnehmer in diesem Sinne gilt jede natürliche oder juristische Person, die mit einem Anbieter von Telekommunikationsdiensten einen Vertrag über die Erbringung derartiger Dienste geschlossen hat.[857] Da in den meisten Fällen über ein dem Arbeitnehmer zur Verfügung gestelltes Mobiltelefon gerade der Arbeitgeber mit dem Diensteanbieter einen Vertrag geschlossen haben wird, ist der Arbeitgeber hier auch als Teilnehmer ein-

---

855 So *Buchner*, DuD 2015, S. 372–377 (375).
856 Vgl. *Eckhardt* in Heun: Handbuch Telekommunikationsrecht, [2]2007, Kapitel L, Rn. 260.
857 Vgl. § 3 Nr. 20 TKG.

zuordnen. Sofern der Arbeitgeber als Teilnehmer zu qualifizieren ist[858], trifft ihn also die Verpflichtung, den Arbeitnehmer bei der Überlassung der Telekommunikationsmittel auf die von ihm erteilte Einwilligung hinzuweisen.

Sinnvoll erscheint in diesem Zusammenhang jedoch, auch weitere Möglichkeiten zur Standortermittlung im jeweiligen Einzelfall zu prüfen, die weniger weitreichende Verpflichtungen mit sich bringen. Zu denken wäre in diesem Zusammenhang an die Anwendung von GPS zur Ortung.[859] Dies hat den Vorteil einer bis auf wenige Meter genauen Ortung, während bei der Anwendung anderer Techniken, wie z.B. einer Ortung über GSM nur eine Bestimmung der Funkzelle möglich ist, in der sich der Nutzer aufhält.[860] Die Vorschriften des Telekommunikationsgesetzes wären jedoch dabei nicht weiter zu beachten.

(i) Standortdaten

Die Regelung des § 98 Abs. 1 TKG setzt zunächst voraus, dass es sich um Standortdaten aus Diensten mit Zusatznutzen handelt. Nach § 3 Nr. 5 TKG ist davon jeder Dienst umfasst, der die Erhebung und Verwendung von Verkehrsdaten oder Standortdaten in einem Maß erfordert, das über das für die Übermittlung einer Nachricht oder die Entgeltabrechnung dieses Vorganges erforderliche Maß hinausgeht.

Dies betrifft meist sog. Local Based Services als standortbezogene Dienste, die die Position eines Nutzers eines mobilen Endgeräts ermitteln, um sodann auf den jeweiligen Aufenthaltsort zugeschnittene Dienste anbieten zu können, wie dies beispielsweise bei Navigationsdiensten und ortsgebundener Werbung der Fall ist.[861]

Als Standortdaten werden alle Daten verstanden, die in einem Telekommunikationsnetz erhoben oder verwendet werden und die den Standort des Endgeräts eines Endnutzers

---

858 Zur Klärung der Frage, ob es sich bei dem Arbeitgeber um einen Teilnehmer handelt, kann ebenfalls auf die Ausführung zum Telemediengesetz zurückgegriffen werden, vgl. dazu unter *Kapitel 3, Teil 3, III.2.*. Danach der Arbeitgeber als Nutzer des Dienstes zu qualifizieren ist, sofern ihm der Dienst zugutekommt. Die Daten aus solchen Diensten mit Zusatznutzen stehen allein dem Arbeitgeber zur Verfügung. Somit ist auch in Bezug auf die Einstufung des Arbeitgebers als Teilnehmer unter Anwendung der Vorschriften des Telekommunikationsgesetzes darauf abzustellen, dass sich die aus den Diensten ergebenden Daten lediglich auf das Arbeitsverhältnis beziehen mit der Folge, dass allein der Arbeitgeber hier als Teilnehmer einzustufen ist.

859 Vgl. dazu unter *Kapitel 3, Teil 7, III.2.*.

860 Vgl. *Löwnau* in Scheurle/Mayen: Telekommunikationsgesetz, ^{2}2008, § 98, Rn. 8 f..

861 So Tinnefeld/Buchner/Petri: Einführung in das Datenschutzrecht, ^{5}2011, S. 409; vgl. dazu auch unter *Kapitel 3, Teil 3, III.*

eines Telekommunikationsdienstes für die Öffentlichkeit angeben.[862] Dies kann sich insbesondere beziehen auf den Standort des Endgerätes des Nutzers nach geographischer Breite und Höhe, die Übertragungsrichtung, sowie den Grad der Genauigkeit der Standortinformation.[863] Über die Standortdaten lässt sich feststellen, wann sich eine Person an welchem Ort aufgehalten hat und über welchen Zeitraum. Dies greift sehr weit in die Persönlichkeitssphäre des Einzelnen ein.

Insbesondere auch im Arbeitsverhältnis lässt dies Rückschlüsse auf die Person des Nutzers zu, die letztlich wiederum zur Leistungskontrolle herangezogen werden könnten. Deshalb dürfen Standortdaten letztlich nur für solche Dienste verwendet werden, für deren Erbringung der Standort des Nutzers wesensnotwendig ist.[864] Für die Wirksamkeit der erforderlichen Einwilligung kann auf die allgemeinen Grundsätze sowie die Besonderheiten in Bezug auf die Einwilligung im Arbeitsverhältnis verwiesen werden.[865] Möglich ist die Erteilung der Einwilligung auch innerhalb einer Rahmenvereinbarung, sodass es nicht erforderlich ist, dass vor jeder Inanspruchnahme eines Dienstes eingewilligt werden muss.[866]

(ii) Umfang

Vom Umfang her ist die Verwendung von Standortdaten in doppelter Hinsicht beschränkt. Nach § 98 Abs. 1 Satz 1 TKG dürfen die Daten nur im zur Bereitstellung des jeweiligen Dienstes mit Zusatznutzen erforderlichen Maß und zudem nur innerhalb des dafür erforderlichen Zeitraums verwendet werden. Das erforderliche Maß sowie der erforderliche Zeitraum sind anhand einer Einzelfallbetrachtung unter Berücksichtigung der Besonderheiten des jeweiligen Dienstes zu ermitteln.[867]

(iii) Informationspflichten nach § 93 TKG

Im Hinblick auf die Erhebung und Verwendung von Standortdaten ist zu berücksichtigen, dass nach dem Willen des Gesetzgebers die Informationspflichten gemäß § 93

862 Vgl. § 3 Abs. 19 TKG.
863 Vgl. *Braun* in Geppert/Schütz: Beck'scher TKG-Kommentar, [4]2013, § 98, Rn. 1.
864 Vgl. *Fetzer* in Arndt/Fetzer/Scherer: TKG, 2008, § 98, Rn. 7.
865 Vgl. unter *Kapitel 3, Teil 3, II.*.
866 BT-Drs. 15/2361 vom 09.01.2004, S. 89, http://dip21.bundestag.de/dip21/btd/15/023/1502316.pdf.
867 Vgl. *Braun* in Geppert/Schütz: Beck'scher TKG-Kommentar, [4]2013, § 98, Rn. 23.

TKG[868] auch in diesem Fall erfüllt werden müssen. Dabei ist dem Teilnehmer mitzuteilen, welche Arten von Standortdaten verarbeitet werden, für welche Zwecke, wie lange und ob die Daten zum Zwecke der Bereitstellung von Diensten mit Zusatznutzen an einen Dritten weitergegeben werden.[869]

Die dem Teilnehmer nach § 98 Abs. 1 Satz 2 TKG auferlegte Pflicht zur Unterrichtung von weiteren Teilnehmern über die von ihm erteilte Einwilligung erweist sich in der Praxis als schwierig.

Aber auch eine solche Pflicht des Diensteanbieters ließe sich über die allgemeine Vorschrift des § 93 TKG ableiten, indem man diese Information unter das Merkmal des *„Umfangs"* der Verwendung der Daten fassen würde. Eine andere Lösungsmöglichkeit wäre dahingehend denkbar, dass eine solche Hinweispflicht als Teilaspekt der Aufklärungspflicht des Diensteanbieters angesehen wird, die nach § 98 Abs. 1 Satz 1 TKG der Einwilligung des Teilnehmers vorausgehen muss.[870] Dies hätte zur Folge, dass für den Fall des fehlenden Hinweises von einer unwirksamen Erteilung der Einwilligung des Teilnehmers auszugehen wäre.

Zuletzt sei an dieser Stelle darauf hingewiesen, dass ein etwaiger Handel mit Standortdaten als unzulässig angesehen wird. Ein Handel mit Standortdaten ist also grundsätzlich verboten.[871] Dies stellte das Bundeswirtschaftsministerium fest, nachdem bekannt wurde, dass der Mobilfunkanbieter *O2* Bewegungsdaten seiner Kunden zum Verkauf

---

868 Nach § 93 Abs. 1 Satz 1 TKG haben Diensteanbieter ihre Teilnehmer bei Vertragsschluss über Art, Umfang, Ort und Zweck der Erhebung und Verwendung personenbezogener Daten so zu unterrichten, dass die Teilnehmer in allgemein verständlicher Form Kenntnis von den grundlegen Verarbeitungstatbeständen der Daten erhalten. Die Nutzer sind gemäß § 93 Abs. 1 Satz 3 TKG vom Diensteanbieter durch allgemein zugängliche Informationen über die Erhebung und Verwendung personenbezogener Daten zu unterrichten.

869 BT-Drs. 15/2361 vom 09.01.2004, S. 89 http://dip21.bundestag.de/dip21/btd/15/023/1502316.pdf.

870 So *Fetzer* in Arndt/Fetzer/Scherer: TKG, 2008, § 98, Rn. 11.

871 Inzwischen wurde durch den Europäischen Gerichtshof im Zusammenhang mit dem Handeln bzw. der Übertragung solcher Daten eine entsprechende Entscheidung im Hinblick auf Verkehrsdaten getroffen. Mit Urteil vom 22.11.2012 hat der Europäische Gerichtshof entschieden, dass eine Übermittlung von Verkehrsdaten durch den Diensteanbieter an den Zessionar einer Entgeltforderung nur dann rechtmäßig sei, wenn der Diensteanbieter im Hinblick auf die Einziehung seiner die Telekommunikationsleistung betreffenden Forderungen an einen Zessionar dieser Forderung übermittelt und dieser die Daten verarbeiten darf, sofern er in Bezug auf die Verarbeitung dieser Daten auf Weisung des Diensteanbieters handelt und sich auf die Verarbeitung derjenigen Verkehrsdaten beschränkt, die für die Einziehung der abgetretenen Forderung erforderlich sind, vgl. Europäischer Gerichtshof, Urteil vom 22.11.2012, Aktenzeichen C-119/12, NJW 2013, S. 989. Es ist hier jedoch zu differenzieren nach dem Zweck, für welchen die Daten jeweils übermittelt werden sollten. Insoweit wird man eine Übermittlung von Verkehrsdaten im vorliegenden Kontext nicht gleichsetzen können mit einer Übermittlung von Standortdaten zu Werbezwecken. Vgl. näher zur Problematik nur *Eckhardt* in Heun: Handbuch Telekommunikationsrecht., ^{2}2007, Kapitel L, Rn. 262 f..

und zu Werbezwecken nutzen wollte. Eine Ausnahme besteht nur für Dienste mit Zusatznutzen, die beispielsweise Verkehrsströme messen, und in diesen Fällen selbst dann nur, wenn dies anonymisiert oder mit Einwilligung des Teilnehmers erfolge.[872] Es solle verhindert werden, dass durch solche Vermarktungspraktiken der Verletzung der Privatsphäre Tür und Tor geöffnet würden.[873]

2. Ortung

Eine weitere mitbestimmungspflichtige Maßnahme ist in der Ortung von Mitarbeitern[874] zu sehen. Dies betrifft insbesondere extern tätige Arbeitnehmer, die keinen festen Arbeitsplatz innehaben und dadurch als *„mobile"* Arbeitnehmer bezeichnet werden.[875] Die vielfältigen Hintergründe für die Ortung externer Arbeitnehmer können insbesondere in der Kontrolle der vertraglichen Arbeitszeiten, der Einsatzplanung und –koordinierung sowie der Kontrolle eines etwaigen Missbrauchs eines auch für private Zwecke überlassenen Dienstfahrzeugs liegen.[876] Ebenfalls werden Ortungssysteme zur Sicherheit der Arbeitnehmer und der Betriebsmittel des Arbeitgebers eingesetzt.[877]

Näher betrachtet werden sollen an dieser Stelle einerseits der Einsatz von Ortungssystemen zur Einsatzplanung und zum Flottenmanagement sowie andererseits der Einsatz derselben zur Diebstahlsicherung.

a) Flottenmanagement

Im Bereich des Flottenmanagements kommt es dem Arbeitgeber vorwiegend darauf an, die Flotte den Einsätzen entsprechend einsetzen und steuern zu können. Dabei ist es für den Arbeitgeber von besonderer Bedeutung, auf aktuelle Gegebenheiten oder Änderungen schnell und effektiv reagieren zu können. Aber auch innerhalb des Flottenmanagements werden vom Arbeitgeber häufig verschiedene Zwecke verfolgt. Während es dem

---

872 Vgl. http://www.handelsblatt.com/unternehmen/it-medien/ortungsprogramm-bundesregierung-verbietet-o2-handel-mit-bewegungsdaten/7328904.html.

873 Vgl. http://www.zeit.de/digital/mobil/2012-10/bewegungsdaten-verkauf-verbot.

874 Hinsichtlich der technischen Ausgestaltung muss hier unterstellt werden, dass die sich durch die Anwendung von GPS ergebenden Daten automatisch an den Arbeitgeber weitergeleitet werden.

875 So *Gola*, NZA 2007, S. 1139–1144 (1139).

876 Vgl. *Byers* in Weth: Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2014, S. 324.

877 Dabei soll durch die Ortungsmaßnahmen die Verkehrssicherheit durch die Kontrolle von Fahrt- und Ruhezeiten erhöhen und in besonders gefahrgeneigtem Arbeitsumfeld die persönliche Sicherheit der Arbeitnehmer gewährleisten. Zudem sind darunter auch die Fälle zu fassen, in denen es dem Arbeitgeber darauf ankommt, präventiv gegen Straftaten durch Dritte gegen Arbeitnehmer oder Betriebsmittel des Arbeitgebers gerichtet vorzugehen, vgl. dazu insgesamt *Byers* in Weth: Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2014, S. 327 ff.

Arbeitgeber sowohl darauf ankommen kann, durch die Ortung die Einsatzplanung für die Arbeitnehmer effektiv zu gestalten, kann es andererseits auch Zweck der Ortung sein, die Einhaltung der Arbeitszeit durch die Arbeitnehmer zu kontrollieren. Dies spielt insbesondere im Bereich der Entgeltabrechnung gegenüber Kunden eine Rolle. Es soll dadurch ermöglicht werden, anhand der gefahrenen Kilometer und der dokumentierten Arbeitszeit dem Kunden eine nachvollziehbare und prüffähige Abrechnung zu überlassen.

b) Diebstahlsicherung

Oftmals werden Ortungssysteme jedoch auch im Bereich der Diebstahlsicherung eingesetzt.

Mit der Vorschrift des § 32 Abs. 1 Satz 2 BDSG wird eine Datenverwendung zur Aufdeckung von Straftaten erlaubt, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Datenverwendung zur Aufklärung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Datenverwendung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Obwohl dies nicht eindeutig aus der Vorschrift des § 32 BDSG hervorgeht, beurteilt sich die Zulässigkeit von präventiven Maßnahmen zur Abwehr von Straftaten nach § 32 Abs. 1 Satz 1 BDSG, der hierbei in Zusammenhang mit der Vorschrift des § 32 Abs. 1 Satz 2 BDSG steht und aufgrund dessen ebenfalls die danach notwendige Verhältnismäßigkeitsprüfung vorzunehmen ist.[878]

Eine Ortung darf in diesen Fällen allerdings nur innerhalb der Arbeitszeit erfolgen. Im Hinblick auf die Aufdeckung von konkreten Straftaten gilt § 32 Abs. 1 Satz 2 BDSG. Notwendig ist dabei ein konkreter Tatverdacht. Es müssen Tatsachen vorliegen, die Indizien für das Vorliegen eines Straftatbestandes erfüllen.[879] Zudem muss die Datenverwendung zu diesem Zweck erforderlich sein. Weniger intensive Eingriffe dürfen

878 Vgl. *Thüsing*, NZA 2009, S. 865–870 (868).
879 Vgl. *Gola/Schomerus*: BDSG, [12]2015, § 32, Rn. 41.

nicht möglich sein.[880] Zuletzt sind auch hierbei die im Einzelfall vorliegenden gegenseitigen Interessen gegeneinander abzuwägen.

c) Bewegungsprofile über GPS-Anwendung

Aufgrund der bereits entwickelten Technik ist es schon zum jetzigen Zeitpunkt möglich, über GPS-Anwendung ein Kraftfahrzeug bis auf wenige Meter genau zu orten und sich über Bluetooth in das Kraftfahrzeug zu schalten. Zudem ermöglicht der Einsatz von Ortungssystemen die Dokumentation der zurückgelegten Strecke und der aktuellen Position. Dies führt dazu, dass anhand dieser Daten umfassende Bewegungsprofile des Arbeitnehmers erstellt werden können. Außendienstmitarbeitern wird dadurch ihre relative Autonomie genommen, wenn ihr jeweiliger Aufenthaltsort sekundengenau bestimmbar ist.[881]

Darin ist mit der Rechtsprechung des Bundesarbeitsgericht eine besondere Gefährdung des Persönlichkeitsrechts zu sehen, wenn auf diese Weise ununterbrochen eine ungleich größere Anzahl von Daten erhoben werden könne als bei der Überwachung durch Menschen und darüber hinaus die Abläufe der technisierten Datenermittlung für den Arbeitnehmer nicht durchschaubar seien.[882]

Vor diesem Hintergrund sind auch GPS-Geräte als technische Überwachungseinrichtungen einzustufen mit der Folge, dass in diesen Fällen wiederum der Tatbestand des § 87 Abs. 1 Nr. 6 BetrVG greift und somit ein Mitbestimmungsrecht des Betriebsrats angenommen werden muss.[883]

d) Informationspflichten nach §§ 98, 93 TKG

Im Hinblick auf die bereits im Zusammenhang mit der Übertragung von Standortdaten erwähnte Informationspflicht nach §§ 98, 93 TKG weist der Gesetzgeber in Bezug auf Ortungsdienste auf die Missbrauchsgefahr hinsichtlich der sensiblen Daten hin und mahnt, dass dem einwilligenden Teilnehmer zukünftig deutlicher vor Augen geführt werden müsse, dass er die Feststellung des Standortes seines Mobilfunkendgerätes er-

---

880 Vgl. *Seifert* in Simitis: Bundesdatenschutzgesetz, [8]2014, § 32, Rn. 105.

881 So *Däubler*: Gläserne Belegschaften, [6]2015, Rn. 318.

882 Bundesarbeitsgericht, Beschluss vom 08.11.1994, Aktenzeichen 1 ABR 20/94, NZA 1995, S. 313-314 (313).

883 Arbeitsgericht Kaiserslautern, Beschluss vom 27.08.2008, Aktenzeichen 1 BVGa 5/08, BeckRS 2010, 73916; vgl. auch Klebe in DKKW: BetrVG, [14]2014, § 87, Rn. 197, 202; *Däubler*: Das Arbeitsrecht 1, [16]2006, Rn. 985a.

mögliche.[884] Dem trägt auch die besondere Informationspflicht nach § 98 Abs. 1 Satz 3 TKG Rechnung. Danach hat der Anbieter des Dienstes mit Zusatznutzen bei jeder Feststellung des Standortes des Mobilfunkendgerätes den Nutzer durch eine Textmitteilung an das Endgerät, dessen Standortdaten ermittelt wurden, zu informieren. Etwas anderes gilt nur, soweit der Teilnehmer einer Zusendung von Mitteilungen widersprochen hat.[885]

e) Anwendung der Grundsätze zur Videoüberwachung

Es existiert bislang allerdings kein gesetzlicher Tatbestand, der die Zulässigkeit des Einsatzes von Ortungssystemen regelt.

Jedoch besteht insoweit Einigkeit, dass sich die Zulässigkeit von Ortungsmaßnahmen an den allgemeinen datenschutzrechtliche Grundsätzen sowie für den Fall der heimlichen Ortung an der zur Videoüberwachung entwickelten Rechtsprechung zu orientieren hat.[886] Auch dabei spielt der Aspekt des gläsernen Arbeitnehmers eine Rolle. Denn ein Arbeitnehmer wäre schnell *„gläsern"*, wenn er während seiner gesamten Tätigkeit gefilmt würde.[887] In jeden Fall unverhältnismäßig ist jedwede Videoüberwachung im Kernbereich privater Lebensführung.[888]

(i) Öffentliche zugängliche Plätze

Die Videoüberwachung an öffentlich zugänglichen Plätzen[889] richtet sich dabei nach § 6b BDSG. An öffentlich zugänglichen Arbeitsplätzen ist mithin eine offene Videoüberwachung problemlos möglich und zulässig. Obwohl auch die offene Videoüberwachung beim Arbeitnehmer einen Überwachungsdruck hervorruft, kann sich der Arbeitnehmer in dieser Situation darauf einstellen und sein Verhalten anpassen.

Aber auch die heimliche Videoüberwachung in öffentlich zugänglichen Räumen wird nach der Rechtsprechung des Bundesarbeitsgerichts nicht als ausnahmslos unzulässig

---

884 BT-Drs. 16/12405 vom 24.03.2009, S. 15, http://dip21.bundestag.de/dip21/btd/16/124/1612405.pdf.

885 Vgl. § 95 Abs. 2 Satz 2 TKG.

886 Vgl. *Raif*, *ArbR-Aktuell* 2010, S. 359–362 (360); *Däubler*: Gläserne Belegschaften, [6]2015, Rn. 321; *Byers* in Weth: Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2014, S. 327; *Wedde* in DKWW: Bundesdatenschutzgesetz, [4]2014, § 32, Rn. 106.

887 So *Joussen*, NZA-Beilage 2011, S. 35–42 (35).

888 Darunter fallen z.B. Sanitäranlagen und Umkleiden, vgl. *Forst* in Auernhammer: BDSG, [4]2014, § 32 BDSG, Rn. 87.

889 Ein Raum ist als öffentlich zugänglich einzustufen, wenn er nach seinem Zweck dazu dient, von unbestimmt vielen oder nach allgemeinen Merkmalen bestimmten Personen betreten zu werden, vgl. *Byers* in Weth: Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2014, S. 344.

angesehen, sondern vielmehr auf einzelne Ausnahmefälle zu beschränken sein.[890] Dies lässt sich auch durch eine verfassungskonforme Auslegung des § 6b BDSG begründen. Denn danach erfordert die Zulässigkeitsprüfung immer eine Interessenabwägung, die jedoch bei der Annahme eines ausnahmslosen Verbots der heimlichen Videoüberwachung unterlaufen würde.[891] Aber auch in diesem Fällen muss ein nach § 6b Abs. 1 BDSG normierter Zweck gegeben sein. Zudem ist auch an dieser Stelle die Erforderlichkeit zu prüfen sowie eine Verhältnismäßigkeitsprüfung vorzunehmen.

(ii) Nicht öffentliche zugängliche Plätze

Die Videoüberwachung an nicht öffentlich zugänglichen Arbeitsplätzen beurteilt sich nach den allgemeinen Grundsätzen. Denn eine direkte Anwendung des § 6b BDG scheidet ebenso aus wie eine analoge Anwendung desselben. Es sind für letzteren Fall nach der Gesetzesbegründung spezielle Regelungen erforderlich.[892] Mithin fehlt es in diesem Fall an einer für die Annahme einer Analogie notwendigen planwidrigen Regelungslücke. Auch an dieser Stelle muss jedoch zwischen offener und heimlicher Videoüberwachung differenziert werden. Die Zulässigkeit der offenen Videoüberwachung in nicht öffentlich zugänglichen Räumen beurteilt sich auf Grundlage der Rechtsprechung des Bundesarbeitsgerichts[893] maßgeblich nach der Intensität des Eingriffs im Rahmen der Prüfung der Angemessenheit der Maßnahme. Dabei ist insbesondere auf die Anzahl der beobachteten Personen, die Dauer der Überwachung sowie darauf abzustellen, ob die Betroffenen einen zurechenbaren Anlass für ihre Beobachtung gesetzt haben, was letztlich auf eine Interessenabwägung hinausläuft.[894]

Auch im Bereich der öffentlich zugänglichen Räume kann in Bezug auf die heimliche Videoüberwachung nichts anderes gelten als für die Videoüberwachung in nicht öffentlich zugänglichen Räumen. Ein Ausschluss jeglicher heimlicher Videoüberwachung würde die Durchsetzung der Interessen des Arbeitgebers regelrecht umfassend verhindern. Insoweit muss eine heimliche Videoüberwachung möglich sein, allerdings gemessen an den Voraussetzungen des § 32 Abs. 1 Satz 2 BDSG. Es muss der konkrete Ver-

890 Bundesarbeitsgericht, Urteil vom 27.03.2003, Aktenzeichen 2 AZR 51/02, NZA 2003, S. 1193-1196.

891 So *Byers* in Weth: Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2014, S. 348.

892 BT-Drs. 14/4329 vom 13.10.2000, S. 38, http://dipbt.bundestag.de/doc/btd/14/043/1404329.pdf.

893 Bundesarbeitsgericht, Beschluss vom 29.06.2004, Aktenzeichen 1 ABR 21/03, NZA 2004, S. 1278-1284; Bundesarbeitsgericht, Beschluss vom 14.12.2004, Aktenzeichen 1 ABR 34/03, NJOZ 2005, S. 2708-2717; Bundesarbeitsgericht, Beschluss vom 26.08.2008, Aktenzeichen 1 ABR 16/07, NZA 2008, S. 1187-1194.

894 Vgl. *Thüsing/Forst*, RDV 2011, S. 163–170 (169).

dacht einer Straftat bestehen und die Videoüberwachung das einzige Mittel sein, um den Täter überführen zu können. Aber auch im Bereich der Videoüberwachungstechnik schreitet die Entwicklung derart voran, dass es über sog. *„Thinking Cameras"* mittlerweile möglich ist, mit Hilfe entsprechender Software die Bilder anhand vorgegebener Muster zu durchsuchen und Konsequenzen aus den Ergebnissen herzuleiten.[895]

(iii) Übertragung der Grundsätze auf den Einsatz von Ortungssystemen

Diese Grundsätze sind auf die Fälle des Einsatzes von Ortungssystemen zu übertragen. Im Zusammenhang mit der Ortung von Arbeitnehmern über GPS ist in vielen Fällen die Ausstattung des externen Arbeitnehmers mit einem Mobiltelefon als milderes Mittel anzusehen. Darüber können die Arbeitnehmer bei bestehendem Anlass auf dem dienstlichen Mobiltelefon angerufen und nach ihrem Standort befragt werden.[896] Eine reine Arbeitszeitkontrolle über sog. GPS-Tracking ist auch in den Fällen als unverhältnismäßig anzusehen, in denen die Auswertung reiner Kilometerstände ausreichend erscheint.[897]

Es ist jedoch trotz alledem zu beachten, dass auch eine zulässige Ortung der Arbeitnehmer letztlich nur in Maßen erfolgen sollte. Beispielsweise darf die nach § 28 Abs. 1 Nr. 2 BDSG zulässige Ortung zum Zweck des Diebstahlschutzes letztlich nicht übermäßig sein. Denn eine schrankenlose Rechtfertigung lässt sich in diesen Fällen nicht allein daraus ableiten, dass es sich bei den zu schützenden Gegenständen um Eigentum des Arbeitgebers handelt. Dazu hat das Bundesarbeitsgericht wie folgt entschieden:

> *„Wird die Videoüberwachung im privaten Bereich nicht heimlich, sondern sichtbar durchgeführt, so hat der Besucher grundsätzlich die Möglichkeit, der Überwachung durch Fernbleiben von den überwachten Räumen zu entgehen. Verbleibt er gleichwohl freiwillig, wird darin regelmäßig seine Einwilligung zu sehen sein. Der Arbeitnehmer hat diese Möglichkeit nicht. Er hat gerade die Pflicht, sich am Arbeitsplatz aufzuhalten, um dort seine geschuldete Arbeitsleistung zu erbringen. Er kann sich deshalb der Überwachung durch Verlassen der Räumlichkeiten nicht entziehen. Hinzu kommt, dass auch der Arbeitgeber verpflichtet ist, den Arbeitnehmer vertragsgemäß zu beschäftigen. Sein Hausrecht unterliegt aus diesen Gründen einer Einschränkung. Er kann die Videoüberwa-*

895 Vgl. *Oberwetter*, NZA 2008, S. 609–613 (610).
896 Vgl. LfD Rheinland-Pfalz: 22. Tätigkeitsbericht 2008-2009, S. 64, http://www.datenschutz.rlp.de/downloads/tb/tb22.pdf.
897 Vgl. *Jaspers/Franck*, RDV 2015, S. 69–73 (73).

chung nicht allein damit rechtfertigen, es handele sich um „seine" Räumlichkeiten."[898]

Dies bestätigt wiederum die strenge Zwecksetzung, dass eine lückenlose Überwachung durch den Arbeitgeber verhindert werden soll. Allerdings besteht für den Arbeitgeber auch die Möglichkeit, eine wirksame Einwilligung des Arbeitnehmers einzuholen, welche die Datenverwendung sodann erlaubt. Aber auch an dieser Stelle sei auf die Problematik der Freiwilligkeit der Einwilligung im Arbeitsverhältnis verwiesen.[899]

Die Thematik der Ortungssysteme wird in der Datenschutz-Grundverordnung zumindest indirekt aufgegriffen. Nach Art. 22 DS-GVO hat eine natürliche Person das Recht, nicht einer auf einer rein automatisierten Verarbeitung von Daten basierenden Maßnahme unterworfen zu werden, die ihr gegenüber rechtliche Wirkungen entfaltet oder sie in maßgeblicher Weise beeinträchtigt und deren Zweck in der Auswertung bestimmter Merkmale ihrer Person oder in der Analyse beziehungsweise Voraussage etwa ihres Aufenthaltsorts oder ihres Verhaltens besteht. Dies soll nach Art. 22 Abs. 2 DS-GVO nur möglich sein, wenn die Datenverwendung im Rahmen des Abschlusses oder der Erfüllung eines Vertrages vorgenommen wird, dies ausdrücklich aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten gestattet ist oder eine Einwilligung hierzu erteilt wurde.

Aufgrund der Tatsache, dass eine Ortung in nahezu keinem denkbaren Fall der Erfüllung des Arbeitsvertrages dienen wird und auch hierbei im Hinblick auf die Freiwilligkeit einer im Arbeitsverhältnis erteilten Einwilligung des Arbeitnehmers Bedenken bestehen[900], wird letztlich auf seitens des nationalen Gesetzgebers zu erlassende Rechtsakte dazu abgestellt werden müssen, welche Profilingmaßnahmen, insbesondere auch zur Ermittlung des Aufenthaltsorts, im dafür erforderlichen Maß als zulässig einstufen.

3. Fahrtenschreiber

Auch hinsichtlich des Einsatzes von Fahrtenschreiber muss ein Mitbestimmungsrecht letztlich angenommen werden.

---

898 Bundesarbeitsgericht, Beschluss vom 14.12.2004, Aktenzeichen 1 ABR 34/03, NJOZ 2005, S. 2708-2717 (2714).

899 Vgl. unter *Kapitel 3, Teil 3, II.3.b).*

900 Vgl. unter *Kapitel 3, Teil 3, II.3.b).*

Der Fahrtenschreiber stand als erste Generation von Kontrolleinrichtungen im Blickpunkt, auf den der Gesetzgeber mit der Regelung des § 87 BetrVG abzielte.[901]

Die Frage, ob über den Einbau bzw. die Verwendung eines Fahrtenschreibers der Betriebsrat mitzuentscheiden hat, ist gerade im vorliegenden Kontext relevant. Denn hier muss differenziert werden zwischen dem gesetzlich vorgeschrieben Einbau derselben in LKW[902] und dem freiwilligen Einbau durch den Arbeitgeber in Leichtfahrzeuge. Aber auch in letztgenanntem Fall fällt ein Fahrtenschreiber nach der Rechtsprechung des Bundesarbeitsgerichts als technische Einrichtung im Sinne des § 87 Abs. 1 Nr. 6 BetrVG unter den Tatbestand und löst ein Mitbestimmungsrecht des Betriebsrates aus.[903] Denn der Fahrtenschreiber sei danach objektiv dazu geeignet, das Verhalten oder die Leistung des Arbeitnehmers zu überwachen. Nur sofern die Anbringung und Verwendung von Fahrtenschreibern gesetzlich vorgesehen sei, bestehe kein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG. Beim Einsatz von Fahrtenschreiber wird also auch dann ein Mitbestimmungsrecht bejaht, wenn der Einbau bzw. die Verwendung nicht gesetzlich vorgeschrieben ist.

Allerdings ist an dieser Stelle darauf hinzuweisen, dass der Einbau von Fahrtenschreibern gleich welcher Art[904] teilweise kritisch beurteilt wird. In diese Richtung äußerte sich auch der damalige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Peter Schaar im Jahr 2006. Dabei konstatierte er, dass der Einsatz solcher Geräte nur vertretbar sei, wenn die nachfolgenden datenschutzrechtlichen Anforderungen erfüllt seien:

- *„Ein verpflichtender Einbau der „Event Data Recorder“ sollte nur bei besonders gefahrgeneigten Transporten (...) vorgesehen werden. (...)*
- *(...), dass auf Kfz-Halter und Fahrer auch kein ökonomischer Zwang ausgeübt wird – etwa durch Versicherungsgesellschaften. (...) (keine Dauerüberwachung am Arbeitsplatz)*

---

901 Vgl. *Klebe* in DKKW: BetrVG, [14]2014, § 87, Rn. 167.

902 Vgl. § 57a StVZO. Danach sind mit einem nach dem Mess- und Eichgesetz in Verkehr gebrachten Fahrtschreiber Kraftfahrzeuge mit einem zulässigen Gesamtgewicht von 7,5 t und darüber sowie Zugmaschinen mit einer Motorleistung von 40 kW und darüber, die nicht ausschließlich für land- oder forstwirtschaftliche Zwecke eingesetzt werden, auszurüsten. Dies gilt nach § 57a Abs. 1 Satz 2 StVZO jedoch nicht für Kraftfahrzeuge mit einer durch die Bauart bestimmten Höchstgeschwindigkeit von nicht mehr als 40 km/h.

903 Bundesarbeitsgericht, Beschluss vom 10.07.1979, Aktenzeichen 1 ABR 50/78, DB 1979, S. 2428-2429 (2428).

904 Darunter fallen unter anderem der verpflichtend im LKW einzubauende Fahrtenschreiber, der Unfalldatenschreiber sowie der Event Data Recorder.

- *(...) Dabei ist sicherzustellen, dass eine gegenseitige Kontrolle von verschiedenen Nutzern eines Fahrzeugs oder durch den Halter – (...) – unterbleibt.“*[905]

Der Einwand, ein verpflichtender Einbau von Event Data Recorder solle nur bei besonders gefahrgeneigten Transporten vorgesehen werden, ist im Lichte der heutigen technischen Entwicklung neu einzuschätzen. Durch die gesetzlich vorgeschriebene Verpflichtung zum Einbau des eCall-Systems in Neufahrzeuge ab März 2018[906] wird dies erweitert. Ein verpflichtender Einbau ist dann nicht mehr nur für Gefahrguttransporter oder Busse vorgeschrieben, sondern auch für private Leichtkraftfahrzeuge. Dies rechtfertigt sich jedoch dadurch, dass Untersuchungen und Studien zufolge die Zahl der Verkehrstoten so um ein Vielfaches reduziert werden kann.

Auch der Forderung, dass es zu keiner Dauerüberwachung von Arbeitnehmern komme dürfe und eine solche ausgeschlossen werden müsse, ist hier die mittlerweile rasant vorangeschrittene Technik entgegenzustellen. Die Forderung muss hier zwar aufrechterhalten werden. Dies ist Sinn und Zweck der Vorschriften des Bundesdatenschutzgesetzes. Jedoch besteht eine Technik zur Dauerüberwachung bereits und kann auch eingesetzt werden.

Ähnlich ist dies auch im Hinblick auf die Telematik-Branche zu beurteilen. Die Forderung, dass durch Versicherungen kein ökonomischer Zwang erzeugt werden dürfe, kann nur solange bestehen bleiben, bis in der Sparte der Telematik-Anbieter eine dahingehende Entwicklung stattfinden wird. Dies ist zu befürchten. Eine gesetzliche Regelung, die ein solches Verhalten verbieten würde, existiert bislang nicht.

Zuletzt ist auch der Aspekt einer zu verhindernden gegenseitigen Kontrolle der Fahrzeugnutzer untereinander oder durch den Halter neu zu beurteilen. Hierbei kann eine gegenseitige Kontrolle bzw. eine Kontrolle durch den Halter insbesondere im Rahmen der Telematik- und Big Data-Anwendungen in Betracht kommen. Darüber ist es heutzutage technisch möglich, ein vollständiges Bewegungsprofil des Fahrers zu generieren.

---

905 So Peter Schaar auf einem internationalen Workshop der Europäischen Akademie für Informationsfreiheit und Datenschutz zum Thema *„Vehicle Event Recording and Data Protection“* am 28.03.2006 in Berlin, vgl. http://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2006/PM-13-06Schaar-AbsageAnDenGlaesernenAutofahrer.html?nn=5217154. Ähnlich äußerte er sich auch im Rahmen eines Vortrages bei einem ADAC-Fachgespräch am 28.09.2006 in München, vgl. http://www.bfdi.bund.de/DE/Infothek/Reden_Interviews/2006/GlaesernerAutofahrerUnterGeneralverdacht.html?nn=5217192.

906 Vgl. unter *Kapitel 2, Teil 5, III.*.

Pflichten, den Fahrer oder andere Nutzer darüber zu informieren, ergeben sich bislang lediglich aus vertraglichen Informationspflichten.

Insoweit sind die von *Schaar* aufgestellten Forderungen an die nunmehr vorliegenden technischen Gegebenheiten anzupassen. An der Tatsache, dass in Bezug auf freiwillig seitens des Arbeitgebers anzuwendende Fahrtenschreiber ein Mitbestimmungsrecht des Betriebsrates nach § 87 Abs. 1 Nr. 6 BetrVG besteht, ändert sich dadurch jedoch nichts. Vielmehr muss dem technischen Fortschritt und den sich daraus ergebenden Möglichkeiten Einhalt geboten werden, indem dabei technisch-organisatorischen Maßnahmen erforderlich werden.

Teil 8: Technische und organisatorische Maßnahmen nach § 9 BDSG

Als letzter Schritt ist es zur Umsetzung der vorgenannten datenschutzrechtlichen Grundlagen für die Implementierung technischer Systeme zur Vernetzung von Fahrzeugen untereinander und mit Verkehrseinrichtungen insbesondere in den vorgenannten praktisch relevanten Fällen zwingend notwendig, dass sich die Einführung und Anwendung derselben als technische und organisatorische Maßnahmen an den Grundsätzen der Vorschrift des § 9 BDSG zu messen haben.

Darüber muss letztlich gewährleistet werden, dass trotz der voranschreitenden Technik die Einhaltung der datenschutzrechtlichen Vorschriften sichergestellt wird.

Die Vorschrift des § 9 BDSG[907] nebst Anlage trifft explizite Regelungen zur Datensicherheit bzw. Datensicherung im Regelungsbereich des Bundesdatenschutzgesetzes. Die Datensicherung umfasst die Gesamtheit aller organisatorischen und technischen (nicht rechtlichen) Regelungen und Maßnahmen, mit denen ein unzulässiger Umgang mit personenbezogenen Daten zu verhindern und die Integrität sowie Verfügbarkeit der Daten und die zu deren Verarbeitung eingesetzten technischen Einrichtungen zu erhal-

[907] Neben einigen bereichsspezifischen Vorschriften, wie insbesondere § 78a SGB X und § 109 TKG existieren vielfach Verweisungen auf § 9 BDSG mit rein deklaratorischem Charakter, wie beispielsweise § 9 Antiterrordateigesetz, § 9 Refinanzierungsregisterverordnung und § 7 Deckungsregisterverordnung. Aber auch in den jeweiligen Landesdatenschutzgesetzen finden sich entsprechende Regelungen. Diese sind Art. 7 BayDSG, § 10 BbgDSG, § 5 BlnDSG, § 7 BremDSG, § 10 DSG-LSA, § 21 DSG-MV, § 10 DSG-NW, § 10 HDSG, § 8 HmbgDSG, § 9 LDSG-BW, § 9 LDSG-RP, § 5 LDSG-SH, § 7 NDSG, § 9 SächsDSG, § 11 SDSG, § 9 ThürDSG. Vgl. dazu *Schmieder* in Forgó: Betrieblicher Datenschutz, 2014, S. 897.

ten ist.[908] Durch diese Maßnahmen soll insbesondere die Vertraulichkeit gewährleistet werden. Aufgrund von technischem Versagen, Unachtsamkeit oder auch durch vorsätzliche Handlungen besteht jedoch im Hinblick auf die Datensicherung die inhärente Gefahr, dass dadurch die Vertraulichkeit beeinträchtigt wird.[909] Dies soll durch die Maßnahmen nach § 9 BDSG nebst Anlage verhindert werden. Die verantwortliche Stelle hat auf Grundlage der Regelungen in § 9 BDSG ein einheitliches Sicherheitskonzept zu erstellen und umzusetzen.[910] Allerdings hat es der Gesetzgeber aufgrund der Vielzahl der möglichen Einzelfallkonstellationen unterlassen, die zu treffenden Maßnahmen genau zu beschreiben und stattdessen in der Anlage zu § 9 BDSG lediglich diejenigen Maßnahmen aufgelistet, die mindestens zu beachten sind.[911] Dabei ist der Begriff der *„technischen und organisatorischen Maßnahmen"* weit auszulegen und umfasst alle Maßnahmen, die geeignet sind, den Regelungszweck der Norm, also die Sicherung der Daten und der zu ihrer Verarbeitung eingesetzten Prozesse zu unterstützen.[912]

I. Technische und organisatorische Maßnahmen im Sinne des § 9 BDSG iVm Anlage zu § 9 Satz 1 BDSG

Nach § 9 Satz 1 BDSG haben öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführungen der Vorschriften des Bundesdatenschutzgesetzes, insbesondere die in der Anlage zum Bundesdatenschutzgesetz genannten Anforderungen zu gewährleisten. Erforderlich sind in diesem Sinne die Maßnahmen, die nach einer Verhältnismäßigkeitsprüfung als angemessen einzustufen sind. Der Aufwand der Maßnahmen muss in einem angemessenen Verhältnis zu dem angestrebten Zweck stehen.[913] Dabei ist vorwiegend auf die Schutzbedürftigkeit der einzelnen gespeicherten Daten abzustellen.[914] Die Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der dabei anfallenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken

---

908 Vgl. *Ernestus* in Simitis: Bundesdatenschutzgesetz, [8]2014, § 9, Rn. 2.

909 Vgl. Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz Kataloge, [14. EG]2014, G 5.71 Vertraulichkeitsverlust schützenswerter Informationen, S. 1124, https://gsb.download.bva.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2014_EL14_DE.pdf.

910 So *Gola/Klug*: Grundzüge des Datenschutzrechts, 2003, S. 100.

911 Vgl. *Plath* in Plath: BDSG, 2013, § 9, Rn. 2.

912 Vgl. *Schultze-Melling* in Taeger/Gabel: BDSG, [2]2013, § 9 BDSG, Rn. 20.

913 Vgl. § 9 Satz 2 BDSG.

914 So *Gola/Schomerus*: BDSG, [12]2015, § 9, Rn. 9.

und der Art der zu schützenden personenbezogenen Daten angemessen ist.[915] Im Rahmen einer Risikoanalyse von möglichem Schadenseintritt und Eintrittswahrscheinlichkeit sollten Anhaltspunkte für die Verhältnismäßigkeit von Maßnahmen gefunden und bei der Planung konkreter Sicherheitsmaßnahmen berücksichtigt werden.[916]

Nach Satz 1 und Satz 2 der Anlage zu § 9 Satz 1 BDSG ist die betriebliche Organisation im Falle der automatisierten Verarbeitung oder Nutzung von personenbezogenen Daten so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind, eine der Nr. 1 bis Nr. 8 der Anlage zu § 9 Satz 1 BDSG zu erfüllen. Hierbei ist jedoch zu beachten, dass es sich bei den dort genannten Aspekten nicht um Maßnahmen technischer oder organisatorischer Art handelt, sondern dass darin lediglich Anforderungen im Sinne von Zielvorgaben enthalten sind, die den Einsatz besonderer Datenschutzmaßnahmen erfordern und die erfüllt werden müssen.[917] Insoweit sind die Maßnahmen nur in ihrem Ergebnis verbindlich, während hinsichtlich der Form der Umsetzung ein weiter Entscheidungsspielraum seitens der verantwortlichen Stelle besteht.[918]

II. Weitergabekontrolle

Für die Beurteilung von notwendigen technischen und organisatorischen Maßnahmen im Zusammenhang mit dem Einsatz vernetzter Fahrzeuge im Arbeitsverhältnis soll durch die Weitergabekontrolle nach Nr. 4 der Anlage zu § 9 Satz 1 BDSG gewährleistet werden, dass auch im Rahmen der elektronischen Übertragung oder des Transports des Datenträgers auf die personenbezogenen Daten nicht unbefugt zugegriffen werden kann.[919] Dies umfasst das unbefugte Lesen, Kopieren, Verändern oder Entfernen der personenbezogenen Daten. Einer unbefugten Kenntnisnahme durch *„Lesen“* kann softwaretechnisch dadurch begegnet werden, dass durchgängig sichere Verschlüsselungsverfahren angewendet werden.[920] Zudem können nicht hinreichend kontrollierbare

915 Vgl. Erwägungsgrund (83) DS-GVO sowie Erwägungsgrund (46) DS-RL.
916 Vgl. *Schmieder* in Forgó: Betrieblicher Datenschutz, 2014, S. 898.
917 Vgl. *Ambs* in Erbs: Strafrechtliche Nebengesetze, [201. EL]2015, § 9 BDSG, Rn. 5.
918 Vgl. *Karg* in Wolff/Brink: Datenschutzrecht in Bund und Ländern, 2013, BDSG Anlage, Rn. 7.
919 Vgl. *Wächter*: Datenschutz im Unternehmen, [4]2013, Rn. 749.
920 Sog. „*Ende-zu-Ende-Verschlüsselung*“, vgl. Wedde in Däubler/Klebe/Wedde/Weichert: Bundesdatenschutzgesetz, [4]2014, § 9, Rn. 67.

Schnittstellen durch entsprechende technische Maßnahme geschlossen werden.[921] Damit kann eine Einwirkung in vorgenannter Form verhindert werden.

Durch die Übermittlungskontrolle als Teilaspekt der Weitergabekontrolle soll als vorbeugende Maßnahme die Prüfbarkeit der Datenübermittlung gesichert werden.[922] Nach Nr. 4 der Anlage zu § 9 Satz 1 BDSG muss überprüft oder festgestellt werden können, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Eine solche Feststellung ist durch Protokollierung der Übertragungsvorgänge zu ermöglichen. Aufgrund des eindeutigen Wortlauts ist jedoch lediglich durch Protokollierung darzustellen, welche Übermittlung an wen *„vorgesehen"* ist. Es sind danach also nicht sämtliche Übertragungsvorgänge zu protokollieren, aus denen sich ergeben würde, an wen eine Übermittlung erfolgt *„ist"*. Aus der Protokollierung muss ersichtlich sein, an welche Stelle, in welcher Menge und in welchem zeitlichen Rahmen eine Übermittlung vorgesehen ist.[923] Da hierbei jedoch wegen der protokollierten personenbezogenen Daten die Möglichkeit besteht, Verstöße aufzudecken und den Verantwortlichen heranzuziehen, muss hier eine Aufbewahrungsfrist festgelegt werden, nach deren Ablauf die Daten zu löschen sind. Dabei ist in Bezug auf die Protokolle eine kurze Aufbewahrungsfrist von einem Jahr einzuhalten.[924]

In Satz 3 der Anlage zu § 9 Satz 1 BDSG[925] ist unter anderem für die Nr. 4 der Anlage zu § 9 Satz 1 BDSG als Maßnahme die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren vorgesehen. Durch Verschlüsselung der Informationen lassen sich letztlich die Schutzziele der Vertraulichkeit und Integrität verwirklichen.[926] Es ist mithin erforderlich, eine durchgängige Verschlüsselung sicher zu gewährleisten. Damit ist sichergestellt, dass die verantwortliche Stelle selbst die Herr-

---

921 Vgl. *Schultze-Melling* in Taeger/Gabel: BDSG, [2]2013, § 9 BDSG, Rn. 66.

922 Vgl. *Ambs* in Erbs: Strafrechtliche Nebengesetze, [201. EL]2015, § 9 BDSG, Rn. 11.

923 Vgl. *Ernestus* in Simitis: Bundesdatenschutzgesetz, [8]2014, § 9, Rn. 119 ff.

924 Vgl. Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz Kataloge, [14. EG]2014, M 2.110, Datenschutzaspekte bei der Protokollierung, S. 1632, https://gsb.download.bva.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2014_EL14_DE.pdf; vgl. ebenso Gutting/Sicking in Weth: Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2014, S. 589.

925 Das Erfordernis der Verschlüsselung findet sich zudem in einzelnen Landesdatenschutzgesetzen sowie in bereichsspezifischen Gesetzen, wie z.B. § 87a Abs. 1 AO und § 6 DIMDIV.

926 Vgl. *Karg* in Wolff/Brink: Datenschutzrecht in Bund und Ländern 2013, BDSG Anlage, Rn. 44.

schaft über die Daten behält. Dies ist auch beim Einsatz von End- und Speichergeräten, wie z.B. Notebooks und mobilen Festplatten, Tablets oder Smartphones zu beachten.[927]

Sofern auch Daten aus dem Kraftfahrzeug beispielsweise direkt an den Hersteller übertragen werden, sind die vorgenannten Grundsätze ebenfalls zu beachten. Dies gilt insbesondere auch für die erforderliche Protokollierung der Übertragungswege.

Beim Autohersteller Daimler wird dies beispielsweise durch das sog. *„Daimler Vehicle Backend"* verwirklicht. Dabei werden die Daten zunächst anonymisiert und erst danach an den jeweiligen Diensteanbieter übertragen, während im Rahmen der sicherheitsrelevanten Car to X-Kommunikation auf eine pseudonymisierte Kommunikation gesetzt wird, um die Herkunft falscher, missbräuchlich abgesetzter Verkehrsinformationen auf diese Weise leichter und schneller aufklären zu können, als dies im Fall der Anonymisierung möglich wäre.[928]

III. Eingabekontrolle

Über die Eingabekontrolle ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind. Ziel der Eingabekontrolle ist die Nachvollziehbarkeit des Datenverarbeitungsvorgangs.[929]

Im Gegensatz zur Weitergabekontrolle nach Nr. 4 der Anlage zu § 9 Satz 1 BDSG soll hier im Rahmen der Nr. 5 der Anlage zu § 9 Satz 1 BDSG eine ex-post-Betrachtung ermöglicht werden. Dies erfordert eine umfassende Protokollierung. Unter Protokollierung in diesem Zusammenhang versteht man die Erstellung von manuellen oder automatisierten Aufzeichnungen, durch welche sich beantworten lässt, wer, wann, mit welchen Mitteln was veranlasst bzw. worauf zugegriffen hat.[930] Um feststellen zu können, wer die Eingabe vorgenommen hat, muss die Möglichkeit einer genauen Identitätsbestimmung des Verantwortlichen bestehen, welcher in der Lage ist, bei der Eingabe in das Datenverarbeitungssystem auf den Inhalt der Daten einzuwirken oder die Entscheidung über die Eingabe zu treffen.[931] Es ist hier nicht ausreichend, lediglich einen mögli-

---

927 Vgl. *Schmieder* in Forgó: Betrieblicher Datenschutz, 2014, S. 905.
928 Vgl. *Schwartmann*, Sonderveröffentlichung zu RDV 3/2015, S. 4.
929 Vgl. *Schmieder* in Forgó: Betrieblicher Datenschutz, 2014, S. 906.
930 So *Karg* in Wolff/Brink: Datenschutzrecht in Bund und Ländern, 2013, BDSG Anlagen, Rn. 28.
931 Vgl. *Ambs* in Erbs: Strafrechtliche Nebengesetze, [201. EL]2015, § 9 BDSG, Rn. 12.

chen Personenkreis zu benennen.[932] Die Angabe einer Auswahl an möglichen Personen genügt insoweit nicht. Dies verdeutlicht den präventiven Charakter der Maßnahme. Denn sie erzeugt einen Überwachungsdruck bei den Betroffenen, der sie dazu anhält, nur im Rahmen der ihnen zugewiesenen Aufgaben auf Daten und Systeme zuzugreifen.[933] Die Betroffenen wissen um die Protokollierung und die Tatsache, dass ihr Verhalten festgehalten wird. Dies führt dazu, dass sie bereits im Vorhinein Überlegungen anstellen, um ihr Handeln innerhalb des Arbeitsverhältnisses anzupassen.

Im Zusammenhang mit der Protokollierung ist jedoch auch zu jedem Zeitpunkt der Grundsatz der Datenvermeidung und Datensparsamkeit nach § 3a BDSG zu beachten. Damit so wenige Daten wie möglich verwendet werden, ist insbesondere auf die in § 3a Satz 2 BDSG genannten Methoden der Anonymisierung und der Pseudonymisierung abzustellen.[934]

Dies gilt insbesondere im Arbeitsverhältnis. Die protokollierten Daten des Arbeitnehmers sind im Hinblick auf dessen Recht auf informationelle Selbstbestimmung hier auf ein Minimum zu reduzieren. Dies ist notwendig, um die gegenläufigen Interessen des Arbeitgebers an der Protokollierung einerseits und des Arbeitnehmers am Schutz seiner personenbezogenen Daten andererseits auszugleichen. Dabei ist zu berücksichtigen, wie viele Personen tatsächlich die entsprechenden Daten verarbeiten. Je umfangreicher eine Protokollierung jedenfalls erfolgt, umso höher steigt das Risiko, dass es infolgedessen zu einer ungewollten und unzulässigen Verhaltens- und Leistungskontrolle kommt.[935] Auch deshalb sind in Bezug auf die Protokollierung ebenfalls Erforderlichkeit und Angemessenheit der Protokollierung zu beachten. Auch die Protokolldaten sind wiederum nach den Vorgaben der Anlage zu § 9 Satz 1 BDSG zu sichern und insbesondere der Kreis der Zugriffsberechtigten auf ein Mindestmaß einzuschränken.[936]

Auf Grundlage des Grundsatzes der Zweckbindung wird eine konkrete Festlegung des Zwecks der Nutzung der Protokolldaten im Vorfeld der Maßnahme verlangt, wie dies im Arbeitsverhältnis beispielsweise zur Kontrolle der Einhaltung dienst- oder arbeits-

---

932 Vgl. *Gutting/Sicking* in Weth: Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2014, S. 589.
933 Vgl. *Karg* in Wolff/Brink: Datenschutzrecht in Bund und Ländern, 2013, BDSG Anlage, Rn. 30.
934 So *Bizer*, DuD 2006, S. 270–273 (271).
935 Vgl. *Wedde* in DKWW: Bundesdatenschutzgesetz, [4]2014, § 9, Rn. 81; *Plath* in Plath: BDSG, 2013, § 9, Rn. 47; *Wedde*, DuD 2007, S. 752–755 (753); *Leopold*, DuD 2006, S. 274–276 (275).
936 Vgl. *Schmieder* in Forgó: Betrieblicher Datenschutz, 2014, S. 906 f..

rechtlicher Vorgaben möglich ist.[937] Diese strenge Zweckbindung ist gesetzlich in § 31 BDSG geregelt. Danach dürfen personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, auch nur für diese Zwecke verwendet werden. Möglich ist lediglich, den Zweck der Verwendung der Protokolldaten vorab z.B. auf die angemessene Auswertung für Leistungsbeurteilungen auszudehnen.[938] Eine nachträgliche Zweckänderung ist damit ausgeschlossen.

Um diese Anforderungen zu erfüllen, empfiehlt es sich, seitens der verantwortlichen Stelle bei Datenverarbeitungen für mehrere Kunden und auch bei unterschiedlicher Zielsetzung der Datenverarbeitungsprozesse jeweils getrennte Datenverarbeitungsprozesse zu schalten und zu verwalten. Dies erscheint zwar im Hinblick auf den Grundsatz der Datensparsamkeit zunächst nicht schlüssig, erklärt sich jedoch damit, dass durch die vorgenannten Maßnahmen jeweils Manipulationen vermieden werden können.

Erforderlich ist insoweit durch den Arbeitgeber insbesondere im Hinblick auf die Datenverwendung aus dem vernetzten Fahrzeug die Implementierung automatischer oder manueller Protokollierungs- und Archivierungsfunktionen, die ebenfalls auf mobilen Datenverarbeitungsanlagen installiert werden müssen.[939] Auch hierbei ist von einer Aufbewahrungszeit der Protokolle von einem Jahr auszugehen.

Zu beachten ist jedoch letztlich auch ein unter Umständen bestehendes Mitbestimmungsrecht des Betriebsrates gemäß § 87 Abs. 1 Nr. 6 BetrVG hinsichtlich der Protokollierung nach Nr. 4 und Nr. 5 der Anlage zu § 9 Satz 1 BDSG.[940] Aufgrund der Tatsache, dass die notwendigen Maßnahmen grundsätzlich zur Leistungs- und Verhaltenskontrolle eingesetzt werden können und somit nachvollziehbar würde, wann ein Arbeitnehmer beispielweise mit dem Dienstfahrzeug außerhalb der ihm erteilten Befugnisse unterwegs wäre, sind in besonderem Maß der Angemessenheitsgrundsatz sowie die Mitbestimmungsrechte des Betriebsrats zu beachten.[941]

---

937 Vgl. *Knorr*, DuD 2006, S. 268–269 (268).
938 So *Leopold*, DuD 2006, S. 274–276 (276).
939 Vgl. *Plath* in Plath: BDSG, 2013, § 9, Rn. 45.
940 So *Schultze-Melling* in Taeger/Gabel: BDSG, [2]2013, § 9 BDSG, Rn. 67; *Klebe* in DKWW: Bundesdatenschutzgesetz, [4]2014, § 9, Rn. 76, 84; a.A. vgl. *Kort*, NZA 2011, S. 1319–1324 (1322).
941 Vgl. *Schmieder* in Forgó: Betrieblicher Datenschutz, 2014, S. 906.

IV. Datenschutz-Richtlinien und Arbeitsanweisungen

Die Umsetzung der notwendigen technischen und organisatorischen Maßnahmen erfolgt regelmäßig über die Implementierung und Einführung von Richtlinien und Arbeitsanweisungen im Betrieb des Arbeitgebers.

Wegen der technischen Entwicklung hin zu tragbaren Datenträgern und zur Integration von Speichermedien in tragbare Gerät, wie beispielsweise die Integration von Smartphones und Laptops in vernetzten Fahrzeugen muss eine effektive Datenträgerkontrolle in der Praxis durch Implementierung von Arbeitsrichtlinien erreicht werden.[942] Die Implementierung von Arbeitsanweisungen und Arbeitsrichtlinien zum Umgang mit personenbezogenen Daten der Arbeitnehmer ist als organisatorische Maßnahme nach § 9 BDSG zu verstehen. So kann eine Arbeitsanweisung bzw. Arbeitsrichtlinie dergestalt formuliert sein, dass beispielsweise eine Dokumentationspflicht für die Fälle besteht, in denen sich aus dem Verhalten der Arbeitnehmer tatsächliche Anhaltspunkte für den Verdacht ergeben, der Betroffene habe im Arbeitsverhältnis eine Straftat begangen. Eine solche Dokumentationspflicht folgt auch bereits aus dem gesetzlichen Wortlaut.[943] Der Nachweis von Anhaltspunkten, die auf die Begehung einer Straftat hindeuten, kann somit nur erbracht werden, wenn die Tatsachen ausreichend und hinreichend dokumentiert werden.

Im Zusammenhang mit der Datenverwendung aus vernetzten Fahrzeugen und der Vielzahl der durch Big Data-Anwendungen neu zu generierenden Daten müssen die technischen Systeme unter das bestehende Regelungsgefüge subsumiert werden.

Die Datensicherheit als Schutzzweck der Regelung des § 9 BDSG muss dabei bei solch komplexen technischen Systemen durch datenschutzfreundliche Gestaltung *(„Privacy by Design")* und Grundeinstellungen *(„Privacy by Default")* optimiert verwirklicht werden.[944] Durch *„Privacy by Default"* sollen dabei bereits in der Phase der Entwicklung von Anwendungen proaktiv die mit der späteren Nutzung verbundenen datenschutzrechtlichen Anforderungen berücksichtigt werden, während durch die Grundsätze des *„Privacy by Design"* erreicht werden soll, dass Nutzer darauf vertrauen können, dass die grundsätzlichen Datenschutzanforderungen an die jeweilige Anwendung von

---

942 So *Plath* in Plath: BDSG, 2013, § 9, Rn. 42.

943 Vgl. § 32 Abs. 1 Satz 2 BDSG.

944 Vgl. Weichert, Thilo: Datenschutz im Auto - Teil 2. Das Kfz als großes Smartphone mit Rädern. In: *SVR* 2014, S. 241–247(244).

der ersten Nutzung an gewahrt sind und selbst für den Fall, dass die vorgegebenen Werkseinstellungen zunächst nicht geändert werden bzw. die technische Ausgangskonfiguration genutzt wird.[945] Auch ohne Änderung der Einstellungen muss die Anwendung für den Nutzer bereits sicher anwendbar sein. Dies ist auch in Art. 25 DS-GVO vorgesehen. Das Prinzip des *„Privacy by Design"* ist insoweit auch im Wirtschaftsleben anerkannt.[946]

Allerdings fehlen insoweit greifbare Handlungsvorgaben. Es ist den jeweiligen verantwortlichen Stellen selbst überlassen, die notwendigen Maßnahmen zu ergreifen und umzusetzen. Die Maßgaben in § 9 BDSG sowie der dazugehörigen Anlage sind allerdings wenig greifbar. Dies scheint zwar auf den ersten Blick für die Verantwortlichen günstig zu sein, steht ihnen doch mehr oder weniger die entsprechende Umsetzung der erforderlichen Maßnahmen frei. Dies führt jedoch letztlich vielmehr dazu, dass die Anwendung des Verhältnismäßigkeitsgrundsatzes kein einheitliches Ergebnisse liefert. Lediglich unverhältnismäßige und unwirtschaftliche Maßnahmen können darüber ausgeschlossen werden.

Dabei stellt sich jedoch im Anschluss die Frage, wann von einer Unverhältnismäßigkeit auszugehen ist. Im Ergebnis überwiegen hier die unbestimmten Anknüpfungspunkte, die es den verantwortlichen Stellen in der Praxis schwer machen, die richtigen Maßnahmen einzuführen und umzusetzen.

Die Umsetzung der geforderten technischen und organisatorischen Maßnahmen bei der Anwendung intelligenter Verkehrssysteme sowie Big Data im vernetzten Fahrzeug bereitet insbesondere den Arbeitgebern tatsächlich erhebliche Schwierigkeiten. Zunächst fehlt dem Arbeitgeber für nahezu alle aus dem Kraftfahrzeug generierten Daten die Kenntnis darüber, welche Daten überhaupt erhoben, gespeichert oder aber auch an Dritte übermittelt werden.[947] Dem Arbeitgeber fehlt somit bereits der Zugang zu den Daten aus dem vernetzten Fahrzeug und damit zusammenhängender Anwendungen. Zudem muss das Kraftfahrzeug als solches hierbei in die bereits vorhandene Sicherheitskonzeption des Betriebs eingebunden werden, was allerdings die Kenntnis der im Einzelnen

945 Vgl. *Kipker*, DuD 2015, S. 410 (410).

946 Vgl. https://www.vda.de/de/themen/innovation-und-technik/vernetzung/datenschutz-prinzipien-fuer-vernetzte-fahrzeuge.html (dort hinterlegt als pdf).

947 Vgl. unter *Kapitel 3, Teil 6, I.1.*. Die für den Betroffenen geheime Datenverwendung lässt sich hier auch auf die Situation des Arbeitgebers übertragen. Auch ihm gegenüber macht der Hersteller keine Angaben dazu, welche Daten überhaupt erhoben, gespeichert, verarbeitet oder an Dritte übermittelt werden.

ablaufenden Datenverarbeitungsvorgänge im Kraftfahrzeug voraussetzt, die bislang jedoch entweder nicht dokumentiert oder aber als Betriebsgeheimnis von den Herstellern geheim gehalten werden, sodass ein Zugriff Dritter, u.a. des Arbeitgebers, nicht möglich ist.[948] Fehlt es in diesen Fällen an der Kenntnis der technischen Möglichkeiten, um die Daten verwenden zu können, bedingt dies, dass Zielvorgaben nach der Anlage zu § 9 Satz 1 BDSG nicht in Gestalt der dort genannten Maßnahmen umgesetzt werden können. Eine Verschlüsselung als erforderliche Maßnahme nach Nr. 4 der Anlage zu § 9 Satz 1 BDSG kann nicht durchgeführt werden, wenn insoweit das technische Know-How fehlt, um die Daten überhaupt als Arbeitgeber selbst auslesen und verwenden zu können.

Im Ergebnis lassen sich die Möglichkeiten des Arbeitgebers als verantwortlicher Stelle und dessen sich aus § 9 BDSG nebst Anlage ergebenden Pflichten nicht miteinander in Einklang bringen. Dies erfordert Handlungsbedarf. Aufgrund der Tatsache, dass davon auszugehen ist, dass die Hersteller sich trotz dieses offensichtlichen Konflikts in Bezug auf die Gewährleistung eines umfassenden Datenschutzes für den betroffenen Arbeitnehmer als Fahrer nicht von ihrer Argumentation abbringen lassen und auch weiterhin die Erhebung, Speicherung und weitere Verwendung der Daten aus dem vernetzten Fahrzeug als Betriebsgeheimnis zu schützen versuchen werden, kann an dieser Stelle nicht angesetzt werden.

Vielmehr erscheint es notwendig, die Betreiber der verschiedenen Anwendungen zu verpflichten, ihrerseits bereits die erforderlichen und notwendigen technischen und organisatorischen Maßnahmen nach § 9 BDSG zu treffen. Nur so kann sichergestellt werden, dass die Datenverwendung in datenschutzrechtlicher Hinsicht ordnungsgemäß erfolgt.

Auch die Einigung von VDA und den Datenschutzaufsichtsbehörden auf die *„Muster-Information über Datenspeicher im Fahrzeug“*[949] ist im vorliegenden Zusammenhang

948 Vgl. *Kremer*, RDV 2014, S. 240–252 (252).

949 Vgl. http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/Muster-Information_Fahrzeugdatenspeicher.pdf.

als solche organisatorische Maßnahme einzuordnen. Allerdings wurde bereits festgestellt, dass diese Information nicht als ausreichend betrachtet werden kann.[950]

Insgesamt muss festgestellt werden, dass eine umfassende Dokumentation über ein Verfahrensverzeichnis bislang nicht bzw. nur in geringstem Umfang stattfindet. Insoweit ist es dringend erforderlich, dass überhaupt eine Dokumentation vorgenommen wird.

[950] Vgl. unter *Kapitel 3, Teil 6, I.2.*. Dass insoweit eine nicht ausreichende Information vorliegt und gerade nur allgemeine Informationen gegeben werden, verdeutlicht auch eine Aussage des Präsidenten des Bayerischen Landesamtes für Datenschutzaufsicht, Thomas Kranig im Jahr 2012. Er stellte fest, dass sich derjenige, der über diese allgemeinen Informationen hinaus wissen möchte, welche Daten aus seinem Fahrzeug ausgelesen und für welchen Zweck diese Daten verwendet werden, an seine Kfz-Werkstatt oder seinen Fahrzeughersteller wenden müsse, vgl.https://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/Muster-Information_Fahrzeugdatenspeicher.pdf.

Kapitel 4: Zusammenfassung der wesentlichen Ergebnisse und Empfehlungen

Um feststellen zu können, welche Daten in vernetzten Fahrzeugen generiert werden und bei welchen ein Personenbezug bzw. eine Personenbeziehbarkeit in datenschutzrechtlicher Hinsicht angenommen werden muss, ist eine Differenzierung nach fahrzeug- und fahrerbezogenen Sensoren mit und ohne Konfliktpotential vorzunehmen. Während die Daten aus Sensoren mit Konfliktpotential in jedem Fall als personenbezogene Daten einzustufen sind, ist ein Personenbezug auch bei für sich genommen scheinbar belanglosen Daten im Falle der Verknüpfung verschiedener Daten durch Big Data-Anwendung herzustellen. Gleiches gilt für Daten, die aus Fahrerassistenzsystemen generiert werden können.

Durch die Einführung und den Ausbau der Verkehrstelematik findet eine fortschreitende Vernetzung von Kraftfahrzeugen untereinander (Car to Car) sowie mit Elementen der Verkehrsinfrastruktur (Car to Infrastructure) oder anderen Bereichen (Car to X) statt. Dies erleichtert in vielen Bereichen dem Fahrer die Steuerung des Kraftfahrzeugs. Jedoch sollten dabei auch die durch Missbrauch der Systeme zu befürchtenden Gefahren nicht verkannt werden. Durch die Anwendung von Big Data und die Verknüpfung sämtlicher einzeln anfallender und für sich unverfänglicher Daten miteinander kann unter Umständen ein Profil des Fahrers erstellt werden. Diese Gefahren bestehen auch im Hinblick auf die europaweite Einführung des eCall-Systems.

Eine weitere technische Neuerung ist in der Weiterentwicklung des autonomen Fahrens zu sehen. Dem Szenario, die Fahrertätigkeit aus den Händen zu geben, stehen bislang jedoch die Regelungen des *„Wiener Übereinkommens über den Straßenverkehr“* vom 08. November 1968 entgegen. Es bedarf weiterer Änderungen der gesetzlichen Vorschriften, um autonomes Fahren rechtlich möglich zu machen.

Die rechtliche Zulässigkeit einer Verwendung von Daten aus vernetzten Fahrzeugen richtet sich zum jetzigen Zeitpunkt nach den geltenden Vorschriften des Bundesdatenschutzgesetzes und dort insbesondere nach § 4 BDSG sowie den Erlaubnistatbeständen der §§ 28 und 32 BDSG. Daneben haben auch die Vorschriften der zwischenzeitlich auf

europäischer Ebene erlassenen Datenschutz-Grundverordnung auf die nationalen Rechtsvorschriften Einfluss und sind aufgrund des Verordnungscharakters unmittelbar in den Mitgliedstaaten anwendbar.

Im Anwendungsbereich des Bundesdatenschutzgesetzes muss bei der Bestimmung der verantwortlichen Stelle auf die Entscheidungsgewalt über Zweck und Mittel der Datenverwendung abgestellt werden. Die Vernetzung der Kraftfahrzeuge untereinander führt dazu, dass eine Vielzahl an Akteuren beteiligt ist und jeder der Akteure für sich gesehen für einzelne Bereiche der Datenverwendung als verantwortliche Stelle eingeordnet werden kann. Dabei ist für jeden Einzelfall die Herrschaft über die Daten für jede im Kraftfahrzeug gegebene Anwendung maßgeblich. Als verantwortliche Stelle kommen insbesondere Werkstätten, Hersteller, Versicherer und Flottenbetreiber in Betracht.

Der sachliche Anwendungsbereich ist eröffnet, sofern die Daten einen Personenbezug bzw. eine Personenbeziehbarkeit aufweisen. Ein solcher darf im Bereich der Datenverwendung aus vernetzten Kraftfahrzeugen nicht leichtfertig abgelehnt werden. Auch wenn scheinbar nur rein technische Informationen geliefert werden, kann sich auch bereits daraus ein Personenbezug ableiten lassen, wenn beispielsweise Messdaten in einer Werkstatt ausgelesen werden. Einer vorschnellen Ablehnung des Personenbezugs bei technischen Daten ist hier kritisch entgegenzutreten.

Als gesetzliche Erlaubnistatbestände sind im vorliegenden Kontext vor allem die Vorschriften der §§ 28 und 32 BDSG relevant. Im Rahmen des § 28 BDSG ist zu beachten, dass die Erlaubnistatbestände des § 28 Abs. 1 Satz 1 Nr. 1 einerseits sowie des § 28 Abs. 1 Satz 1 Nr. 2 und Nr. 3 BDSG nicht nebeneinander anwendbar sind. Im Verhältnis zu § 28 BDSG verdrängt der Erlaubnistatbestand des § 32 BDSG den Erlaubnistatbestand des § 28 Abs. 1 Satz 1 Nr. 1 BDSG und ist insoweit lex specialis. Auch die Erlaubnistatbestände des § 28 Abs. 1 Satz 1 Nr. 2 und Nr. 3 BDSG werden von § 32 BDSG verdrängt, soweit es sich um die Verwendung von Daten für Zwecke des Beschäftigungsverhältnisses handelt. Die Regelungen sind jedoch nebeneinander anwendbar, wenn die Datenverwendung beschäftigungsfremde Zwecke betrifft. Dies erfordert eine klare Formulierung des Gesetzestextes und somit eine Differenzierung zwischen Beschäftigtendaten und sonstigen beschäftigungsfremden Daten, die bislang nicht existiert. Die Datenverwendung ist als erforderlich anzusehen, sofern sie mehr als nützlich, aber weniger als zwingend notwendig ist.

Aber auch Betriebsvereinbarungen und die Vorschriften des Intelligente Verkehrssysteme Gesetzes können als gesetzliche Erlaubnistatbestände im Sinne des § 4 Abs. 1 BDSG herangezogen werden. Allerdings ergeben sich aus den geplanten Neuregelungen in beiden Bereichen Schwierigkeiten. Betriebsvereinbarungen sind in Art. 6 DS-GVO als Erlaubnistatbestand nicht vorgesehen und auch Art. 88 DS-GVO stellt keine Ermächtigungsgrundlage dar. Auch das Verhältnis der Erlaubnistatbestände der § 3 Satz 2 IVSG sowie § 4 Abs. 1 BDSG zueinander im Hinblick auf die auf einer Einwilligung basierenden Datenverwendung ist bislang nicht eindeutig geklärt. Es besteht Handlungsbedarf.

Die Zulässigkeit der Datenverwendung kann sich auch aus der Erteilung einer wirksamen Einwilligung ergeben. Im Zusammenhang mit vernetzten Fahrzeugen ist dabei aber die Problematik zu beachten, dass Halter und Fahrer nicht identisch sein müssen und zudem ein Kraftfahrzeug von mehreren Fahrern genutzt werden kann. Die Einwilligung muss in diesen Fällen von jedem Einzelnen wirksam erteilt werden, was wiederum in jedem Einzelfall eine freie und informierte Erklärung erfordert. Wie in diesen Fällen die Einwilligung wirksam erteilt bzw. vom Halter eingeholt werden kann, wird die weitere technische Entwicklung zeigen.

Auf europäischer Ebene ist nach Art. 7 DS-GVO sowie Erwägungsgrund (43) DS-GVO vorgesehen, dass eine Einwilligung im Abhängigkeitsverhältnis aufgrund der sodann fehlenden Freiwilligkeit nicht wirksam erteilt werden kann. Eine einmal erteile Einwilligung im Arbeitsverhältnis sollte im vorliegenden Zusammenhang aufgrund der fortschreitenden technischen Entwicklung nach 1 ½ Jahren auf ihre Gültigkeit überprüft werden.

Auf die öffentlich diskutierte Frage, wem Daten aus Kraftfahrzeugen gehören, ist klarzustellen, dass es ein Eigentum an Daten nicht gibt. Diese Fragestellung ist auch nicht als richtiger Anknüpfungspunkt zu sehen. Vielmehr muss eine Zuordnung der Daten zu Einzelnen erfolgen und daraus eine Zugriffsbefugnis abgeleitet werden.

Mangels spezialgesetzlicher Vorschriften kann sich eine Zugriffsbefugnis aus den allgemeinen Vorschriften des Datenschutzrechts ergeben. Es ist zwar nicht möglich, aus sachenrechtlichen Vorschriften über das Eigentum an Datenträgern auch eine Zugriffsbefugnis auf die sich darauf befindenden Daten abzuleiten. Allerdings kann sich aus einer vertragsrechtlichen Zuordnung von Daten eine Zugriffsbefugnis ergeben. Gleiches

gilt für eine Zuordnung über den Bereich des Strafrechts mit Blick auf den Tatbestand des § 202a StGB. Obgleich sich aus den Vorschriften des Urheberrechts keine eigentümerähnliche Stellung ableiten lässt, könnte auch über die dortigen Regelungen eine Zuordnung der Daten erfolgen, was letztlich auch für die datenschutzrechtlich relevanten Vorschriften gilt. Insgesamt können also für Daten an sich kein Eigentum und keine eigentümerähnliche Stellung abgeleitet werden.

Trotzdem ist eine freie Nutzung nicht möglich. Denn aus den vorgenannten Vorschriften und Regelungsbereichen lassen sich eine Zugriffsbefugnis und damit eine rechtliche Zuordnung ableiten. Trotz alledem müssen auch die rechtlich freien Daten berücksichtigt werden, für die keine Zugriffsbefugnis eines einzelnen besteht. Hinsichtlich derer kann sich eine faktische Herrschaftsposition daraus ergeben, dass Fahrzeughaltern zwar die tatsächliche Verfügungsgewalt zuzusprechen ist, diese davon aber wegen eines bei den Herstellern bestehenden Datenmonopols davon keinen Gebrauch machen können. Dem sind jedoch in Bezug auf den Zugang zu Reparatur- und Wartungsinformationen die Vorschriften des Typzulassungsrechts nach der EURO 5/6-Verordnung entgegenzustellen. Daraus ergibt sich die Verpflichtung der Hersteller, jegliche auch nur mittelbar mit der Wartung und Reparatur von Kraftfahrzeugen in Zusammenhang stehende Informationen auf dem freien Markt zur Verfügung stellen zu müssen.

Die Datenverwendung im Kraftfahrzeug findet auf verschiedene Art und Weise statt. Die geheime Datenverwendung erfolgt ohne Einwilligung und ohne Wissen des Betroffenen. Lediglich den Herstellern ist dabei bekannt, welche Daten erhoben, gespeichert oder gar übermittelt werden. Dabei handelt es sich vorwiegend um rein technische Daten hinsichtlich derer dem Betroffenen das nötige Fachwissen fehlt, um die Daten verwenden zu können. Durch Big Data-Anwendung kann aber auch aus diesen Daten ein Rückschluss auf das Verhalten des Betroffenen gezogen werden.

Im Bereich der offiziellen Datenverwendung mit Wissen des Betroffenen ist die Datenverwendung durch die verantwortliche Stelle offenkundig. Dies ist beispielsweise bei der Anwendung von Diensten intelligenter Verkehrssteuerung der Fall. Auch das eCall-System ist unter diese Kategorie zu fassen. Sofern die Datenverwendung im Gegensatz zum eCall-System nicht gesetzlich vorgeschrieben ist, kann eine Aufklärung der Datenverwendung über eine Datenschutzerklärung erfolgen.

Die vom Verband der deutschen Automobilindustrie und den Datenschutzaufsichtsbehörden herausgegebene *„Muster-Information über Datenspeicher im Fahrzeug“* ist jedoch nicht als ausreichende Aufklärung über die Datenverwendung anzusehen. Es fehlt eine Klarstellung darüber, dass auch rein technische Daten an sich bereits fahrerbezogene Informationen liefern und damit zu Konfliktpotential führen können. Dazu ist es gerade nicht notwendig, weitere Informationen, wie z.B. Zeugen oder Unfallprotokolle hinzuzuziehen. Dies geht jedoch aus der Muster-Information nicht hervor.

Zuletzt kann eine Datenverwendung auch mit Einwilligung des Betroffenen stattfinden. Doch auch hier wird wiederum die Problematik relevant, dass es zu einem Kraftfahrzeug mehrere Nutzer gibt und somit die Verpflichtung zur Einholung einer wirksamen Einwilligung ggf. weiterzugeben ist.

Aus der Verwendung von Daten aus vernetzten Dienstfahrzeugen ergibt sich ein Mitbestimmungsrecht des Betriebsrates nach § 87 Abs. 1 Nr. 6 BetrVG für die Einführung technischer Einrichtungen. Lediglich für die Einführung des eCall-Systems ist ein Mitbestimmungsrecht nicht gegeben, weil der Einbau aufgrund gesetzlicher Vorschriften verpflichtend geregelt ist. Für jede sonstige technische Einrichtung im Kraftfahrzeug, welche eine Überwachung der Leistung des Arbeitnehmers ermöglicht, besteht ein Mitbestimmungsrecht. Dies betrifft insbesondere die Anwendung von GPS oder anderer Ortungssysteme sowie die Übertragung von Standortdaten, durch welche sich ein Bewegungsprofil des Arbeitnehmers erstellen lässt. Gemessen an den Grundsätzen zur Videoüberwachung muss die Überwachung streng limitiert werden und einer strengen Zweckbindung unterliegen.

Verschiedene praktische Anwendungsfälle zeigen, dass im Rahmen der Anwendung intelligenter Verkehrssysteme tatsächlich in Bezug auf die Zulässigkeit der Verwendung von Daten aus vernetzten Fahrzeugen auf die Einwilligung des Betroffenen zurückzugreifen sein wird.

Lediglich für die Einführung des eCall-Systems ergibt sich die Zulässigkeit der Datenverwendung aus dem gesetzlichen Erlaubnistatbestand des § 28 Abs. 1 Satz 1 Nr. 2 BDSG.

Im Hinblick auf Regressansprüche des Arbeitgebers gegenüber dem Arbeitnehmer im Falle des Unfalls mit einem Dienstwagen ist danach zu differenzieren, ob es sich um eine rein dienstliche Nutzung des Kraftfahrzeugs handelt oder ob eine private Nutzung

erlaubt ist. In letzterem Fall kann auf den Erlaubnistatbestand des § 28 BDSG zurückgegriffen werden, während im Fall der rein dienstlichen Nutzung als Erlaubnistatbestand lediglich § 32 BDSG in Betracht kommt.

Die Zulässigkeit einer Leistungs- und Verhaltenskontrolle des Betroffenen unter Zuhilfenahme der Daten aus dem Kraftfahrzeug muss sich an § 28 BDSG messen lassen.

Die Datenverwendung zur Verfolgung und Ahndung von Ordnungswidrigkeiten und Straftaten kann nur aufgrund verschiedener Vorschriften der Strafprozessordnung als gesetzliche Erlaubnistatbestände im Sinne des § 4 Abs. 1 BDSG gerechtfertigt werden.

Aufgrund der technischen Weiterentwicklung wird sich zukünftig noch eine Masse an denkbaren Verwendungsmöglichkeiten für Daten aus dem Kraftfahrzeug entwickeln. Dies muss weiter kritisch betrachtet werden.

Aus den vorgenannten Ergebnissen lässt sich ableiten, dass zum jetzigen Zeitpunkt noch eine Vielzahl an Unsicherheiten rechtlicher Art besteht.

Zur Gewährleistung von Datensicherheit und Datensicherung haben die verantwortlichen Stellen die notwendigen technischen und organisatorischen Maßnahmen zu ergreifen. Im Zusammenhang mit der Datenverwendung aus vernetzten Kraftfahrzeugen sind hier insbesondere die Weitergabekontrolle sowie die Eingabekontrolle nach Nr. 4 und Nr. 5 der Anlage zu § 9 Satz 1 BDSG relevant. Beides erfordert eine umfassende Protokollierung der Datenverwendung. Erforderlich ist hierbei eine Implementierung automatischer oder manueller Protokollierungs- und Archivierungsfunktionen durch den Arbeitgeber.

Die Durchführung und Kontrolle dieser Maßnahmen sind in der Praxis durch die Implementierung von Arbeitsanweisungen und Arbeitsrichtlinien zu erreichen. Bei solch komplexen technischen Systemen wie denen der vernetzten Fahrzeuge ist dies bereits durch eine datenschutzfreundlichen Grundeinstellung und Gestaltung über die Grundsätze des *„Privacy by Default“* und des *„Privacy by Design“* sicherzustellen. Dies ist auch in Art. 25 DS-GVO vorgesehen.

Allerdings sind hierbei die daraus für die Arbeitgeber resultierenden Schwierigkeiten zu berücksichtigen im Hinblick darauf, dass ihnen die Kenntnis und die technische Möglichkeit fehlen, um sicherheitsrelevante Datenverarbeitungsvorgänge zu erfassen und daraus notwendige Arbeitsanweisungen entwickeln zu können. Die sich aus § 9 BDSG

samt Anlage für den Arbeitgeber ergebenden Pflichten lassen sich nicht mit dessen Möglichkeiten in Einklang bringen, sodass hier die Betreiber der Anwendungen zu verpflichten sind.

Es bleibt abzuwarten, mit welchem Regelungsgehalt die Vorschriften der Datenschutzgrundverordnung auf den nationalen Beschäftigungsdatenschutz übertragen werden. Die Grenzen des möglichen Regelungsgefüges des nationalen Gesetzgebers müssen sich an der Datenschutzgrundverordnung messen lassen. Grundsätzlich ist wie bereits festgestellt mit Art. 88 DS-GVO eine Öffnungsklausel zugunsten des nationalen Gesetzgebers vorgesehen. Die Auswirkungen sind jedoch bislang nicht absehbar.

Insgesamt muss für den Fahrer vernetzter Fahrzeuge eine selbstbestimmte Nutzung des Kraftfahrzeugs möglich bleiben. Das Recht auf informationelle Selbstbestimmung des Betroffenen muss durch die beteiligten Akteure als verantwortliche Stellen gewährleistet werden. Dies erfordert die Umsetzung verschiedener Empfehlungen, wie diese bereits im Rahmen des 52. Verkehrsgerichtstages 2014 in Goslar sowie im Rahmen der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Oktober 2014 formuliert wurden. Diese können nach dem Ergebnis der vorliegenden Untersuchung aufrechterhalten und wie folgt zusammengefasst werden:

- *Zur Akzeptanz von Innovationen für die Automobilität in Europa muss der Austausch von Daten und Informationen aus dem Fahrzeug Regeln unterworfen werden, die das informationelle Selbstbestimmungsrecht durch Transparenz und Wahlfreiheit des Betroffenen sichern.*
- *Fahrzeughersteller und Dienstleister müssen Käufer bereits bei Vertragsschluss in dokumentierter Form umfassend und verständlich informieren, welche Daten generiert und verarbeitet werden sowie welche Daten auf welchen Wegen und zu welchen Zwecken übermittelt werden. Änderungen dieser Inhalte sind rechtzeitig anzuzeigen. Fahrer sind auf geeignete Weise im Fahrzeug zu informieren. Die Betroffenen müssen in die Lage versetzt werden, weitere Nutzer ebenfalls zu informieren.*
- *Bei der freiwilligen, von einer Einwilligung getragenen oder vertraglich vereinbarten Datenübermittlung an Dritte sind Fahrzeughalter und Fahrer technisch und rechtlich in die Lage zu versetzen, diese zu kontrollieren und ggf. zu unterbinden. Zudem muss Wahlfreiheit für datenschutzfreundliche Systemeinstellungen und die umfangreiche Möglichkeit zum Löschen eingeräumt werden.*

- *Bei Daten, die aufgrund gesetzlicher Regelungen erhoben, gespeichert oder übermittelt werden sollen, sind verfahrensrechtliche und technische Schutzvorschriften zu bestimmen.*
- *Zugriffsrechte der Strafverfolgungsbehörden und Gerichte sind unter konsequenter Beachtung grundrechtlicher und strafprozessualer Schutzziele spezifisch zu regeln.*
- *Bereits in der Konzeptionsphase sind bei der Entwicklung neuer Fahrzeugmodelle und neuer auf Fahrzeuge zugeschnittene Angebote für Kommunikations- und Teledienste die datenschutzrechtlichen Grundsätze des „Privacy by Design" und des „Privacy by Default" zu verwirklichen.*
- *Datenverarbeitungsvorgängen im und um das Fahrzeug muss das Prinzip der Datenvermeidung und Datensparsamkeit zu Grunde gelegt werden. Daten sind in möglichst geringem Umfang zu erheben und umgehend zu löschen, nachdem sie nicht mehr benötigt werden.*
- *Schließlich muss durch geeignete technische und organisatorische Maßnahmen Datensicherheit und Datenintegrität gewährleistet sein. Dies gilt insbesondere für die Datenkommunikation aus dem Kraftfahrzeug heraus.*[951]

Insgesamt sind also die bestehenden Regelungen nicht ausreichend für die Anwendung auf die technische Entwicklung im Bereich vernetzter Fahrzeuge, die derzeit unaufhaltsam weiter voranschreitet.

Insbesondere im Bereich der Transparenz der Datenverwendung für den Betroffenen besteht dringender Handlungsbedarf. Der Fahrer darf das Vertrauen in die technischen Entwicklungen in diesem Bereich nicht verlieren, welche für ihn im jeweiligen Einzelfall günstig sein können. Dem Fahrer bzw. Halter als Betroffenem muss es ermöglicht werden, die Datenverwendung zunächst nachvollziehen und zuletzt steuern zu können. Dabei sind Hersteller, Werkstätten, Flottenbetreiber, Versicherungen und die weiteren Akteure als etwaige verantwortliche Stellen in der Pflicht.

Erforderlich ist eine umfassende und für den Fahrer verständliche Dokumentation und Information über die Datenverwendung. Dies kann nur durch eine noch ausstehende

951 Vgl. dazu insgesamt online unter http://www.gdv.de/wp-content/uploads/2014/01/Verkehrsgerichtstag_2014_Empfehlungen_Arbeitskreis_7.pdf sowie unter https://www.datenschutz-mv.de/datenschutz/themen/beschlue/88_DSK/Ent_Grund.pdf.

feinfühlige Abstimmung der technischen und rechtlichen Regelungswerke gewährleistet werden.

Zudem sollte bereits frühzeitig angesetzt werden bei der Frage nach dem generellen Bedarf an personenbezogenen Daten. Sofern eine Einwilligung des Fahrers vorliegt, muss gewährleistet werden, dass die dort geregelte Datenverwendung jederzeit vom Betroffenen geändert werden können und er selbst dort Veränderungen vornehmen kann.

Im Ergebnis besteht dringender Handlungsbedarf in technischer wie rechtlicher Hinsicht, um die für den Betroffenen notwendige Transparenz für die Datenverwendung herzustellen und Rechtssicherheit zu schaffen.

Literaturverzeichnis

Albrecht, Frank — „Fährt der Fahrer oder das System?“ – Anmerkungen aus rechtlicher Sicht
SVR 2005, S. 373-376

Alpmann / Brockhaus — Fachlexikon Recht, 2004, Münster

Altvater, Lothar
Baden, Eberhard
Berg, Peter
Kröll, Michael
Noll, Gerhard
Seulen, Anna — BPersVG – Bundespersonalvertretungsgesetz, mit Wahlordnung und ergänzenden Vorschriften sowie vergleichenden Anmerkungen zu den Landespersonalvertretungsgesetzen, 8. Aufl. 2013, Frankfurt am Main
(zit. *Bearbeiter* in Altvater: BPersVG)

Ambs, Fritz
Erbs, Georg
Kohlhaas, Max — Strafrechtliche Nebengesetze, Beck`sche Kurzkommentare, Band 17, 201. EL Januar 2015, München
(zit. *Bearbeiter* in Erbs: Strafrechtliche Nebengesetze)

Arndt, Hans-Wolfgang
Fetzer, Thomas
Scherer, Joachim (Hrsg.) — TKG – Telekommunikationsgesetz, Kommentar, 2008, Berlin
(zit. *Bearbeiter* in Arndt/Fetzer/Scherer: TKG)

Auernhammer, Herbert — BDSG – Bundesdatenschutzgesetz und Nebengesetze, Kommentar, 4. Aufl. 2014, Köln
(zit. *Bearbeiter* in Auernhammer: BDSG)

Bach, Markus — Fluch oder Segen?
Auto Zeitung, 11.09.2013 (20/2013), S. 88-89

Bär, Wolfgang — Transnationaler Zugriff auf Computerdaten
ZIS 2011, S. 53-59

Bausewein, Christoph — Legitimationswirkung von Einwilligung und Betriebsvereinbarung im Beschäftigtendatenschutz: Reichweite der Befugnis des Arbeitgebers zur Datenerhebung, -verarbeitung und -nutzung bei Anbahnung und Durchführung des Beschäftigungsverhältnisses, 2012, Edewecht

Bewersdorf, Cornelia	Zur Vereinbarkeit von nicht-übersteuerbaren Fahrerassistenzsystemen mit dem Wiener Übereinkommen über den Straßenverkehr vom 8. November 1968 NZV 2003, S. 266-271
Biegel, Andreas	Überwachung von Arbeitnehmern durch technische Einrichtungen, 2000, Hamburg
Bizer, Johann	Das Recht der Protokollierung DuD 2006, S. 270-273
Bloch, Alexander	Autonomes Fahren: Wer kann was? Auto Motor und Sport, 4/2014, S. 62-69
Boltze, Manfred Wolfermann, Axel (Hrsg.)	Leitfaden Verkehrstelematik, Hinweise zur Planung und Nutzung in Kommunen und Kreisen, 2006, Berlin
Bönninger, Jürgen	Wem gehören die Daten im Fahrzeug? Das moderne Fahrzeug – Messgerät, Steuergerät, Datenspeicher Zfs 2014, S. 184-189
Bouska, Wolfgang	Telematik im Verkehr DAR 1995, S. 353-356
Braess, Hans-Hermann Seiffert, Ulrich (Hrsg.)	Vieweg Handbuch Kraftfahrzeugtechnik, 7. Aufl. 2013, Wiesbaden
Bräutigam, Peter Klindt, Thomas	Digitalisierte Wirtschaft / Industrie 4.0, November 2015
Buchner, Benedikt	Datenschutz im vernetzten Automobil DuD 2015, S. 372-377
Büscher, Wolfgang Dittmer, Stephan Schiwy, Peter	Gewerblicher Rechtsschutz, Urheberrecht, Medienrecht, Kommentar, 3. Aufl. 2015, Köln (zit. *Bearbeiter* in Büscher/Dittmer/Schiwy: Urheberrecht)
Callies, Christian Ruffert, Matthias	EUV, AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, Kommentar, 4. Aufl. 2011, München (zit. *Bearbeiter* in Callies/Ruffert: EUV, AEUV Kommentar)
Daduna, Joachim Rolf Voß, Stefan	Informationsmanagement im Verkehr, 2000, Heidelberg

Däubler, Wolfgang	Das neue Bundesdatenschutzgesetz und seine Auswirkungen im Arbeitsrecht NZA 2001, S. 874-881
Däubler, Wolfgang	Das Arbeitsrecht 1, Leitfaden für Arbeitnehmer, 16. Aufl. 2006, Reinbebek bei Hamburg
Däubler, Wolfgang	Gläserne Belegschaften, Das Handbuch zum Arbeitnehmerdatenschutz, 6. Aufl. 2015, Frankfurt am Main
Däubler, Wolfgang Kittner, Michael Klebe, Thomas Wedde, Peter (Hrsg.)	BetrVG – Betriebsverfassungsgesetz, Kommentar für die Praxis mit Wahlordnung und EBR-Gesetz, 14. Aufl. 2014, Frankfurt am Main (zit. *Bearbeiter* in DKKW: BetrVG)
Däubler, Wolfgang Klebe, Thomas Wedde, Peter Weichert, Thilo	Bundesdatenschutzgesetz, Kompaktkommentar zum BDSG, 4. Aufl. 2014, Frankfurt am Main (zit. *Bearbeiter* in DKWW: Bundesdatenschutzgesetz)
Däubler, Wolfgang Hjort, Peter Schubert, Michael Wolmerath, Martin (Hrsg.)	Arbeitsrecht, Individualarbeitsrecht mit kollektivrechtlichen Bezügen, Handkommentar, 3. Aufl. 2013, Baden-Baden (zit. *Bearbeiter* in DHSW: Arbeitsrecht)
Deutschle, Stephan	„Wer fährt? – Der Fahrer oder das System?“ – Technische Grundlagen von Fahrerassistenzsystemen SVR 2005, S. 249-254
Dorner, Michael	Big Data und Dateneigentum – Grundfragen des modernen Daten- und Informationshandels CR 2014, S. 617-628
Düwell, Franz Josef (Hrsg.)	Betriebsverfassungsgesetz, Handkommentar, 4. Aufl. 2014, Baden-Baden (zit. *Bearbeiter* in Düwell: Betriebsverfassungsgesetz)
Eckhardt, Jens Kramer, Rudi Mester, Britta Alexandra	Auswirkungen der geplanten EU-DS-GVO auf den deutschen Datenschutz DuD 2013, S. 623-630

Ehmann, Horst	Über Datenverarbeitung zur Generalklausel betrieblicher Mitbestimmung – Zugleich kritische Anmerkung zur Kienzle-Schreiber- und zur Opel-PAISY-Entscheidung ZfA 1986, S. 357-401
Eicher, Claus Christoph	Big Brother an Bord ADAC Motorwelt, 4/2014, S. 16-20
Eisenmann, Hartmut Jautz, Ulrich	Grundriss Gewerblicher Rechtsschutz und Urheberrecht, mit 55 Fällen und Lösungen, 9. Aufl. 2012, Heidelberg
Erfurth, René	Der „neue“ Arbeitnehmerdatenschutz im BDSG NJOZ 2009, S. 2914-2927
Fischer, Thomas	Strafgesetzbuch mit Nebengesetzen, Beck`sche Kurzkommentare, Band 10, 61. Aufl. 2014, München
Fitting, Karl Engels, Gerd Schmidt, Ingrid Trebinger, Yvonne Linsenmaier, Wolfgang	Betriebsverfassungsgesetz mit Wahlordnung, Handkommentar, 27. Aufl. 2014, München (zit. *Bearbeiter* in Fitting: Betriebsverfassungsgesetz)
Forgó, Nikolaus Arning, Marian (Hrsg.)	Betrieblicher Datenschutz, Rechtshandbuch, 2014, München
Forst, Gerrit	Videoüberwachung am Arbeitsplatz und der neue § 32 BDSG RDV 2009, S. 204-211
Forst, Gerrit	Beschäftigtendatenschutz im Kommissionsvorschlag einer EU-Datenschutzverordnung NZA 2012, S. 364-367
Forst, Gerrit	Social Media Guidelines. Regelung durch Betriebsvereinbarung? ZD 2012, S. 251-255
Franke, Kai Gonter, Mark Leschke, André Kücukay, Ferit	Steigerung der Fahrzeugsicherheit durch Car2X-Kommunikation ATZ 2012, S. 918-923

Franzen, Martin	Der Vorschlag für eine EU-Datenschutz-Grundverordnung und der Arbeitnehmerdatenschutz Dud 2012, S. 322-326
Franzen, Martin	Beschäftigtendatenschutz: Was wäre besser als der Status quo? RDV 2014, S. 200-202
Freckmann, Anke Störing, Marc Müller, Katharina	Bisherige und zukünftige Bedeutung der Betriebsvereinbarung im Datenschutz verkannt BB 2011, S. 2549-2552
Funke, Thomas	eCall: Lebensretter oder Trojanisches Pferd? Blinklicht 2012, S. 10
Funken, Christian Schulz-Schaeffer, Ingo	Digitalisierung der Arbeitswelt, Zur Neuordnung formeller und informeller Prozesse im Unternehmen, 2008, Wiesbaden
Geiger, Andreas	Die Einwilligung in die Verarbeitung von persönlichen Daten als Ausübung des Rechts auf informationelle Selbstbestimmung NVwZ 1989, S. 35-38
Geppert, Martin Schütz, Raimund	Beck`scher TKG-Kommentar, 4. Aufl. 2013, München (zit. *Bearbeiter* in Geppert/Schütz: Beck`scher TKG-Kommentar)
Gola, Peter	Betrieblicher Datenschutz, Gesetzestext, Erläuterungen und Dokumentation zur Anwendung des BDSG in der betrieblichen Praxis, 1990, Wiesbaden
Gola, Peter	Die Einwilligung als Legitimation für die Verarbeitung von Arbeitnehmerdaten RDV 2002, S. 109-116
Gola, Peter	Datenschutz bei der Kontrolle „mobiler“ Arbeitnehmer – Zulässigkeit und Transparenz NZA 2007, S. 1139-1144
Gola, Peter	Datenschutz am Arbeitsplatz, Handlungshilfen beim Einsatz von Intranet und Internet, E-Mail und Telefon, Big Data und Social Media, 5. Aufl. 2014, Heidelberg
Gola, Peter Klug, Christoph	Grundzüge des Datenschutzrechts, 2003, München

Gola, Peter
Klug, Christoph
Körffer, Barbara
Schomerus, Rudolf
BDSG – Bundesdatenschutzgesetz, Kommentar, 12. Aufl. 2015, München
(zit. *Gola/Schomerus*: BDSG)

Gola, Peter
Wronka, Georg
Handbuch zum Arbeitnehmerdatenschutz, Rechtsfragen und Handlungshilfen für die betriebliche Praxis, 1989, Köln

Gulde, Dirk
Kleine Helfer
Auto Motor und Sport, 26/2013, S. 106-108

Hartmann, Volker
Big Data und Produkthaftung. Produkthaftungsrechtliche Chancen und Risiken des Einsatzes von Big-Data-Technologien im Automobil
DAR 2015, S. 122-126

Hentschel, Peter
König, Peter
Dauer, Peter
Straßenverkehrsrecht, Beck`sche Kurzkommentare, Band 5, 43. Aufl. 2015, München
(zit. *Bearbeiter* in Hentschel: Straßenverkehrsrecht)

Hess, Thomas
Schreiner, Michael
Ökonomie der Privatsphäre. Eine Annäherung aus drei Perspektiven
DuD 2012, S. 105-109

Heun, Sven-Erik (Hrsg.)
Handbuch Telekommunikationsrecht, 2. Aufl. 2007, Köln
(zit. *Bearbeiter* in Heun: Handbuch Telekommunikationsrecht)

Hinrichs, Werner
Personalinformationssystem und Mitbestimmung des Betriebsrats
AuR 1986, S. 285-288

Hoeren, Thomas
Dateneigentum. Versuch einer Anwendung des § 303a StGB im Zivilrecht
MMR 2013, S. 486-491

Hoffmann-Riem, Wolfgang
Informationelle Selbstbestimmung in der Informationsgesellschaft. Auf dem Weg zu einem neuen Konzept für den Datenschutz
AöR 123 (1998), S. 513-540

Hümmerich, Klaus
Boecken, Winfried
Düwell, Franz Josef
AnwaltKommentar, Arbeitsrecht, Band 1, 2. Auflage 2010, Bonn
(zit. *Bearbeiter* in Hümmerich/Boecken/Düwell: Arbeitsrecht)

Jänich, Volker
Schrader, Paul
Reck, Vivien
Rechtsprobleme des autonomen Fahrens
NZV 2015, S. 313-318

Jaspers, Andreas
Franck, Lorenz
Connected Car und Beschäftigtendatenschutz
RDV 2015, S. 69-73

Jauernig, Othmar
Stürner, Rolf (Hrsg.)
BGB – Bürgerliches Gesetzbuch, mit Allgemeinem Gleichbehandlungsgesetz (Auszug), Kommentar, 15. Aufl. 2014, München
(zit. *Bearbeiter* in Jauernig: BGB)

Jentzsch, Nicola
Monetarisierung der Privatsphäre: Welchen Preis haben persönliche Daten?
DIW Wochenbericht, Nr. 34.2014, S. 793-798

Joecks, Wolfgang
StPO – Strafprozessordnung, Studienkommentar, 4. Aufl. 2015, München

Jotzo, Florian
Gilt deutsches Datenschutzrecht auf für Google, Facebook & Co. bei grenzüberschreitendem Datenverkehr?
MMR 2009, S. 232-237

Jourdan, Frank
Matschi, Helmut
Automatisiertes Fahren. Wie weit kann die Technik den Fahrer ersetzen? Entwickler und Gesetzgeber, wer gibt die Richtung vor?
NZV 2015, S. 26-29

Joussen, Jacob
Mitarbeiterkontrolle: Was muss, was darf das Unternehmen wissen?
NZA-Beilage 2011, S. 35-42

Junker, Abbo
Die Entwicklung des Computerrechts in den Jahren 1991 und 1992
NJW 1993, S. 824-832

Kamps, Michael
Das vernetzte Auto als Herausforderung für den Datenschutz
Internationales Verkehrswesen 2014, S. 18-19

Karg, Moritz
Die Renaissance des Verbotsprinzips im Datenschutz
DuD 2013, S. 75-79

Kinast, Karsten
Kühnl, Christina
Telematik und Bordelektronik – Erhebung und Nutzung von Daten zum Fahrverhalten
NJW 2014, S. 3057-3061

Kipker, Dennis-Kenji
Privacy by Default und Privacy by Design
DuD 2015, S. 410

Kirsch, Marcus
Kann der Schutz des BDSG durch Betriebsvereinbarungen unterschritten werden?
MMR-aktuell 2011, 317362

Kittner, Michael
Zwanziger, Bertram
Deinert, Olaf (Hrsg.)
Arbeitsrecht, Handbuch für die Praxis, 7. Auflage 2013, Frankfurt am Main
(zit. *Bearbeiter* in Kittner/Zwanziger/Deinert: Arbeitsrecht)

Klaus, Peter
Krieger, Winfried
Gabler-Lexikon Logistik, Management logistischer Netzwerke und Flüsse, 4. Aufl. 2008, Wiesbaden

Klebe, Thomas
Personaldatenverarbeitung und Verhaltenskontrolle. Zur Auslegung von § 87 Abs. 1 Nr. 6 BetrVG
DB 1986, S. 380-382

Klebe, Thomas
Schumann, Manfred
Die Rechte des Betriebsrats bei der Einführung und Anwendung von Personalinformationssystemen
AuR 1983, S. 40-48

Knorr, Michael
Datenschutzkonforme Protokollierung
DuD 2006, S. 268-269

Kort, Michael
Datenschutzrechtliche und betriebsverfassungsrechtliche Fragen bei IT-Sicherheitsmaßnahmen
NZA 2011, S. 1319-1324

Kremer, Sascha
Connected Car – intelligente Kfz, intelligente Verkehrssysteme, intelligenter Datenschutz?
RDV 2014, S. 240-252

Kroher, Thomas
Digitale Sicherheitslücken, Laptop statt Stemmeisen: BMW-System geknackt
ADAC Motorwelt, 2/2015, S. 20-21

Kudlich, Hans (Hrsg.)
Münchener Kommentar zur Strafprozessordnung, Band 1, §§ 1 – 150 StPO, 1. Aufl. 2014, München
(zit. *Bearbeiter* in Kudlich: MüKo StPO)

Leopold, Nils	Protokollierung und Mitarbeiterdatenschutz. Zielkonflikte im Bundesdatenschutzgesetz DuD 2006, S. 274-276
Lüdemann, Volker Sengstacken, Christin	Lebensretter eCall: Türöffner für neue Telematik Dienstleistungen RDV 2014, S. 177-182
Lutz, Lennart S.	Automatisiertes Fahren: Änderung des Wiener Überein-Kommens tritt im März 2016 in Kraft DAR 2016, S. 55-56
Lutz, Lennart S.	Anforderungen an Fahrerassistenzsysteme nach dem Wiener Übereinkommen über den Straßenverkehr NZA 2014, S. 67-72
Lutz, Lennart S. Tang, Tito Lienkamp, Markus	Die rechtliche Situation von teleoperierten und autonomen Fahrzeugen NZV 2013, S. 57-63
Maunz, Theodor Dürig, Günter	Grundgesetz, Kommentar, 72. EL 2014, München (zit. *Bearbeiter* in Maunz/Dürig: Grundgesetz)
Meyer-Goßner, Lutz Schmitt, Bertram	Strafprozessordnung, Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen, Beck`sche Kurzkommentare, Band 6, 58. Aufl. 2015, München
Mielchen, Daniela	Verrat durch den eigenen PKW – wie kann man sich schützen? SVR 2014, S. 81-87
Möhring, Philipp Nicolini, Käte	Urheberrechtsgesetz – UrhG, KUG, UrhWahrnG, VerlG, Kommentar, 3. Aufl. 2014, München (zit. *Bearbeiter* in Möhring/Nicolini: Urheberrechtsgesetz)
Müller, Reinhold	Das autonome Auto überrollt die Versicherer VW 2013, S. 10
Müller-Glöge, Rudi Preis, Ulrich Schmidt, Ingrid (Hrsg.)	Erfurter Kommentar zum Arbeitsrecht, Beck`sche Kurzkommentare, Band 51, 15. Aufl. 2015, München (zit. *Bearbeiter* in Müller-Glöge/Preis/Schmidt: Erfurter Kommentar zum Arbeitsrecht)

Müllner, Wolfgang	Verhalten und Leistung gemäß § 87 Abs. 1 Nr. 6 BetrVG DB 1984, S. 1677-1680
Oberwetter, Christian	Arbeitnehmerrechte bei Lidl, Aldi & Co. NZA 2008, S. 609-613
Palandt, Otto (Hrsg.)	Bürgerliches Gesetzbuch, Mit Nebengesetzen, Beck`sche Kurzkommentare, Band 7, 74. Aufl. 2015, München (zit. *Bearbeiter* in Palandt/Bassenge: BGB-Kommentar)
Pfeffer, Peter Harrer, Manfred	Lenkungshandbuch, Lenksysteme, Lenkgefühl, Fahrdynamik von Kraftfahrzeugen, 2. Aufl. 2013, Wiesbaden
Philipp, Otmar	Datenschutzrecht: Annahme der Datenschutz-Grundverordnung EuZW 2014, S. 283
Plath, Kai-Uwe (Hrsg.)	BDSG, Kommentar zum BDSG sowie den Datenschutzbestimmungen von TMG und TKG, 2013, Köln (zit. *Bearbeiter* in Plath: BDSG)
Pulathaneli, Timur	Ein offener Ansatz zur App-Integration im Fahrzeug ATZ elektronik 2014, S. 12-17
Raif, Alexander	Beschäftigtendatenschutz: Wird alles neu bei der Arbeitnehmerkontrolle? ArbR-Aktuell 2010, S. 359-362
Redeker, Helmut	Wer ist Eigentümer von Goethes Werther? NJW 1992, S. 1739-1740
Reif, Konrad	Automobilelektronik, Eine Einführung für Ingenieure, 4. Aufl. 2012, Wiesbaden
Reif, Konrad (Hrsg.)	Fahrstabilisierungssysteme und Fahrerassistenzsysteme, 2010, Wiesbaden
Reif, Konrad (Hrsg.)	Sensoren im Kraftfahrzeug, 2010, Wiesbaden
Reif, Konrad (Hrsg.)	Bosch Autoelektrik und Autoelektronik, Bordnetze, Sensoren und elektronische Systeme, 6. Aufl. 2011, Wiesbaden
Richardi, Reinhard (Hrsg.)	Betriebsverfassungsgesetz mit Wahlordnung, Kommentar, 14. Aufl. 2014, München (zit. *Bearbeiter* in Richardi: Betriebsverfassungsgesetz)

Richardi, Reinhard
Wlotzke, Otfried
Wißmann, Hellmut
Oetker, Hartmut (Hrsg.)
Münchener Handbuch zum Arbeitsrecht, Band 1, Individualarbeitsrecht, 3. Auflage 2009, München
(zit. *Bearbeiter* in Richardi/Wlotzke/Wißmann/Oetker: Mü-HB Arbeitsrecht)

Rieger, Frank
Von Daten und Macht
APuZ 15-16/2013, S. 3-7

Riesenhuber, Karl
Die Einwilligung des Arbeitnehmers im Datenschutzrecht
RdA 2011, S. 257-265

Rieß, Joachim
Greß, Sebastian
Privacy by Design für Automobile auf der Datenautobahn
DuD 2015, S. 391-396

Robbers, Gerhard
Der Grundrechtsverzicht. Zum Grundsatz ‚volenti non fit iniuria` im Verfassungsrecht
JuS 1985, S. 925-931

Roberts, Laura
Gabler-Wirtschafts-Lexikon, 17. Aufl. 2010, Wiesbaden

Roßnagel, Alexander
Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, München

Roßnagel, Alexander
Datenschutz in der künftigen Verkehrstelematik
NZV 2006, S. 281-288

Roßnagel, Alexander
Fahrzeugdaten – wer darf über sie entscheiden? Zuordnungen – Ansprüche – Haftung
SVR 2014, S. 281-287

Roßnagel, Alexander
Altenhain, Karsten
Beck`scher Kommentar zum Recht der Telemediendienste, Telemediengesetz, Jugendmedienschutz-Staatsvertrag (Auszug), Signaturgesetz, Signaturverordnung, Vorschriften zum elektronischen Rechts- und Geschäftsverkehr, 2013, München
(zit. *Bearbeiter* in Roßnagel: Beck`scher Kommentar zum Recht der Telemediendienste)

Säcker, Jürgen
Rixecker, Roland
Oetker, Hartmut (Hrsg.)
Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 4, Schuldrecht, Besonderer Teil II, §§ 611-704, EFZG, TzBfG, KSchG, 6. Auflage 2012, München
(zit. *Bearbeiter* in Säcker/Rixecker/Oetker: MüKo BGB)

Säcker, Jürgen
Rixecker, Roland
Oetker, Hartmut (Hrsg.)
Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 6, Sachenrecht, §§ 854-1296, WEG, ErbbauRG, 6. Aufl. 2013, München
(zit. *Bearbeiter* in Säcker/Rixecker/Oetker: MüKo BGB)

Satzger, Helmut
Schluckebier, Wilhelm
Widmaier, Gunter
StPO – Strafprozessordnung, Kommentar, 1. Aufl. 2014, Köln
(zit. *Bearbeiter* in Satzger/Schluckebier/Widmaier: StPO)

Scheurle, Klaus-Dieter
Mayen, Thomas
Telekommunikationsgesetz, Kommentar, 2. Aufl. 2008, München
(zit. *Bearbeiter* in Scheurle/Mayen: Telekommunikationsgesetz)

Schinhammer, Sebastian
Offener Zugang für alle
Autohaus 2012, S. 96-97

Schönke, Adolf
Schröder, Horst
Strafgesetzbuch, Kommentar, 29. Aufl. 2014, München
(zit. *Bearbeiter* in Schönke/Schröder: Strafgesetzbuch)

Schulz, Thomas
Roßnagel, Alexander
David, Klaus
Datenschutz bei kommunizierenden Assistenzsystemen. Wird die informationelle Selbstbestimmung von der Technik überrollt?
ZD 2012, S. 510-515

Schwartmann, Rolf
Datenschutz im gläsernen Auto. Betrieblicher Einsatz von vernetzten Fahrzeugen im Fokus von Datenschutz und Datensicherheit. Tagungsbericht, 16. April 2015
Sonderveröffentlichung zu RDV 3/2015

Schwartmann, Rolf
Ohr, Sara
Datenschutzrechtliche Perspektiven des Einsatzes intelligenter Fahrzeuge
RDV 2015, S. 59-68

Schwarz, Mathias
Das Mitbestimmungsrecht des § 87 Abs. 1 Nr. 6 BetrVG, Eine Zwischenbilanz nach den Beschlüssen des BAG vom 6.12.1983 (Bildschirmarbeitsplatz) und 14.9.1984 (Technikerberichtssystem)
BB 1985, S. 531-535

Schwarz, Mathias
Arbeitnehmerüberwachung und Mitbestimmung, Das Mitbestimmungsrecht des Betriebsrats bei Einführung und Anwendung technischer Einrichtungen der Leistungs- und Verhaltenskontrolle, 1982, Berlin

Seidel, Horst	Grundlagen der Volkswirtschaftslehre, 21. Aufl. 2003, Troisdorf
Shen, Kelei	Augmented Navigation. Verschmelzung von Routen, Karten und Realität ATZ 2013, S. 402-405
Siebenpfeiffer, Wolfgang (Hrsg.)	Vernetztes Automobil, Sicherheit, Car-IT – Konzepte, 2014, Wiesbaden
Simitis, Spiros (Hrsg.)	Bundesdatenschutzgesetz, 8. Aufl. 2014, Baden-Baden (zit. *Bearbeiter* in Simitis: Bundesdatenschutzgesetz)
Spindler, Gerald Schuster, Fabian	Recht der elektronischen Medien, Kommentar, 3. Aufl. 2015, München (zit. *Bearbeiter* in Spindler/Schuster: Recht der elektronischen Medien)
Stephan, M.	So fahren wir in Zukunft Auto BILD Zeitung, 15.06.2014, S. 10
Taeger, Jürgen Gabel, Detlev (Hrsg.)	Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 2. Aufl. 2013, Frankfurt am Main (zit. *Bearbeiter* in Taeger/Gabel: BDSG)
Thüsing, Gregor	Datenschutz im Arbeitsverhältnis. Kritische Gedanken zum neuen § 32 BDSG NZA 2009, S. 865-870
Thüsing, Gregor Forst, Gerrit	Der geplante Beschäftigtendatenschutz: Strenger oder großzügiger als das geltende Recht? RDV 2011, S. 163-170
Tinnefeld, Marie-Theres Buchner, Benedikt Petri, Thomas	Einführung in das Datenschutzrecht, Datenschutz und Informationsfreiheit in europäischer Sicht, 5. Aufl. 2011, München
Wächter, Michael	Datenschutz im Unternehmen, 4. Aufl. 2013, München
Wallentowitz, Henning (Hrsg.)	Handbuch Kraftfahrzeugtechnik, Grundlagen, Komponenten, Systeme, Anwendungen, 1. Aufl. 2006, Wiesbaden
Wandtke, Arthur-Axel Bullinger, Winfried (Hrsg.)	UrhR – Praxiskommentar zum Urheberrecht, 4. Aufl. 2014, München (zit. *Bearbeiter* in Wandtke/Bullinger: Praxiskommentar zum Urheberrecht)

Wandtke, Arthur-Axel (Hrsg.) — Urheberrecht, 4. Aufl. 2014, Berlin (zit. *Bearbeiter* in Wandtke: Urheberrecht)

Wedde, Peter — Die wirksame Einwilligung im Arbeitnehmerdatenschutzrecht DuD 2004, S. 169-174

Wedde, Peter — Protokollierung und Arbeitnehmerdatenschutz DuD 2007, S. 752-755

Weichert, Thilo — Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung NJW 2001, S. 1463-1469

Weichert, Thilo — Datenschutz im Auto – Teil 2. Das Kfz als großes Smartphone auf Rändern SVR 2014, S. 241-247

Weißgerber, Michael — Das Einsehen kennwortgeschützter Privatdaten des Arbeitnehmers durch den Arbeitgeber NZA 2003, S. 1005-1009

Weth, Stephan (Hrsg.) — Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Praxishandbuch zum Arbeitnehmerdatenschutz, 2014, München (zit. *Bearbeiter* in Weth: Daten- und Persönlichkeitsschutz im Arbeitsverhältnis)

Wiese, Günther; Kreutz, Peter; Oetker, Hartmut; Raab, Thomas; Weber, Christoph; Franzen, Martin; Gutzeit, Martin; Jacobs, Matthias — GK-BetrVG, Betriebsverfassungsgesetz, Gemeinschaftskommentar, Band II, §§ 74 – 132, 10. Aufl. 2014, Neuwied (zit. *Bearbeiter* in GK-BetrVG: Betriebsverfassungsgesetz)

Winner, Hermann; Hakuli, Stephan; Wolf, Gabriele (Hrsg.) — Handbuch Fahrerassistenzsysteme, Grundlagen, Komponenten und Systeme für aktive Sicherheit und Komfort, 2. Aufl. 2012, Wiesbaden

Wolff, Heinrich Amadeus; Brink, Stefan — Datenschutz in Bund und Ländern, 2013, München

Wybitul, Tim — Neue Spielregeln für Betriebsvereinbarungen und Datenschutz. BAG schafft Klarheit zu Anforderungen an Umgang mit Arbeitnehmerdaten
NZA 2014, S. 225-232

ZD-aktuell (Hrsg.) — Bundesrat: Intelligente Verkehrssysteme Gesetz gebilligt
ZD-aktuell 2013, 03567

Zech, Herbert — Daten als Wirtschaftsgut – Überlegungen zu einem „Recht des Datenerzeugers“ Gibt es für Anwenderdaten ein eigenes Vermögensrecht bzw. ein übertragbares Ausschließlichkeitsrecht?
CR 2015, S. 137-146

Zilkens, Martin — Datenschutz am Arbeitsplatz
DuD 2005, S. 253-261

Rechtsprechung

Bundesarbeitsgericht

Urteil	02.03.1971	VI ZR 146/69	AP RVO § 637 Nr. 6
Beschluss	09.09.1975	1 ABR 20/74	NJW 1976, 261
Beschluss	10.07.1979	1 ABR 50/78	DB 1979, 2428
Beschluss	22.12.1980	1 ABR 2/79	NJW 1981, 937
Beschluss	06.12.1983	1 ABR 43/81	NJW 1984, 1476
Beschluss	14.09.1984	1 ABR 23/82	NJW 1985, 450
Beschluss	23.04.1985	1 ABR 2/82	NZA 1985, 671
Beschluss	11.03.1986	1 ABR 12/84	NZA 1986, 526
Beschluss	27.05.1986	1 ABR 48/84	NZA 1986, 643
Urteil	22.10.1986	5 AZR 660/85	NZA 1987, 415
Beschluss	27.09.1994	GS 1/89 (A)	NJW 1995, 210
Beschluss	08.11.1994	1 ABR 20/94	NZA 1995, 313
Beschluss	30.08.1995	1 ABR 4/95	NZA 1996, 218
Urteil	07.09.1995	8 AZR 828/93	NZA 1996, 637
Beschluss	20.12.1995	7 ABR 8/95	NZA 1996, 945
Urteil	27.03.2003	2 AZR 51/02	NZA 2003, 1193
Urteil	05.02.2004	8 AZR 91/03	NJW 2004, 2469
Beschluss	29.06.2004	1 ABR 21/03	NZA 2004, 1278
Beschluss	14.12.2004	1 ABR 34/03	NJOZ 2005, 2708
Urteil	18.01.2007	8 AZR 250/06	NZA 2007, 1230
Beschluss	26.08.2008	1 ABR 16/07	NZA 2008, 1187
Urteil	21.06.2012	2 AZR 153/11	NJW 2012, 3594
Beschluss	25.09.2012	1 ABR 45/11	NZA 2013, 275
Vorlagebeschluss	09.07.2013	1 ABR 2/13 (A)	NZA 2013, 1433
Beschluss	10.12.2013	1 ABR 43/12	DuD 2014, 633
Urteil	19.02.2015	8 AZR 1011/13	AuR 2015, 158

Bundesgerichtshof

Urteil	19.01.1955	IV ZR 135/54	NJW 1955, 499
Urteil	17.12.1985	VI ZR 244/84	NJW 1986, 2505
Urteil	04.11.1987	VIII ZR 314/86	NJW 1988, 406
Urteil	18.10.1989	VIII ZR 325/88	NJW 1990, 320
Urteil	14.07.1993	VIII ZR 147/92	NJW 1993, 2436
Urteil	27.03.2007	VI ZR 101/06	NJW 2007, 2558
Urteil	23.06.2009	VI ZR 196/08	NJW 2009, 2888

Beschluss	19.01.2010	StB 27/09	NJOZ 2010, 1274
Urteil	22.12.2011	2 StR 509/10	NJW 2012, 945
Urteil	12.03.2014	IV ZR 295/13	NJW 2014, 1658
Urteil	09.04.2014	VIII ZR 404/12	NJW 2014, 2269
Beschluss	28.10.2014	VI ZR 135/13	GRUR Int. 2015, 296
Beschluss	16.07.2015	4 StR 117/15	NZV 2016, 40

Bundesverfassungsgericht

Teilurteil	05.08.1966	1 BvR 586/62, 610/63, 512/64.	NJW 1966, 1603
Urteil	15.12.1983	1 BvR 209/83	NJW 1984, 419
Beschluss	03.09.1991	2 BvR 279/90	NStZ 1992, 91
Beschluss	18.02.2003	2 BvR 372/01	NStZ-RR 2003, 176
Beschluss	23.01.2004	2 BvR 766/03	NStZ-RR, 143
Beschluss	12.04.2005	2 BvR 1027/02	NJW 2005, 1917
Beschluss	04.04.2006	1 BvR 518/02	NJW 2006, 1939
Beschluss	23.11.2006	1 BvR 1909/06	NJW 2007, 286
Urteil	27.02.2008	1 BvR 370/07, 1 BvR 595/07	NJW 2008, 822
Urteil	02.03.2010	1 BvR 256/08, 263/08, 586/08	NJW 2010, 833

Europäischer Gerichtshof

Urteil	15.12.1976	41/76	NJW 1977, 1007
Urteil	06.11.2003	C-101/01	EuZW 2004, 245
Urteil	29.01.2008	C-275/06	MMR 2008, 227
Urteil	07.05.2009	C-553/07	EuZW 2009, 546
Urteil	24.11.2011	C-70/10	MMR 2012, 174
Urteil	24.11.2011	C-468/10, 469/10	EuZW 2012, 37
Urteil	22.11.2012	C-119/12	NJW 2013, 989
Urteil	13.05.2014	C-131/12	(online)

Sonstige Rechtsprechung

VGH Kassel	Beschluss	14.11.1990	BPV TK 974/90	CR 1991, 745
ArbG Bonn	Beschluss	31.10.2003	2 BVGa 15/03	RDV 2004, 190
LG Berlin	Beschluss	02.07.2004	15 O 653/03	NJW-RR 2004, 1631
OVG Lüneburg	Beschluss	29.01.2007	12 ME 416/06	DAR 2007, 227
BVerwG	Beschluss	16.04.2008	6 P 8.07	PersV 2008, 342

ArbG Kaiserslautern	Beschluss	27.08.2008	1 BVGa 5/08	BeckRS 2010, 73916
LG München	Urteil	08.04.2010	17 HK O 138/10	CR 2011, 830
OLG Frankfurt a.M.	Beschluss	13.07.2010	19 W 33/10	MMR 2010, 792
LAG Hamm	Beschluss	16.09.2011	10 TaBV 17/11	ZD 2012, 183
AG München	Urteil	06.06.2013	343 C 4445/13	NJW-RR 2014, 413
ArbG Frankfurt a.M.	Urteil	08.11.2013	22 Ca 9428/12	(online)
VG Arnsbach	Urteil	12.08.2014	AN 4 K 13.01634	DAR 2014, 663
LG Frankfurt a.M.	Urteil	21.01.2016	2-03 O 505/13	(online)

Lebenslauf

Geburtsdatum	07.02.1987
Geburtsort	55430 Oberwesel
Staatsangehörigkeit	deutsch

1997 – 2006	Wilhelm-Hofmann Gymnasium in St. Goarshausen – Abitur
April 2006	Beginn des Studiums der Rechtswissenschaften an der Johannes Gutenberg-Universität in Mainz
20. Juli 2011	Erstes juristisches Staatsexamen
November 2011	Beginn des Rechtsreferendariats (Koblenz / Frankfurt a.M. / Ingelheim)
21. November 2013	Zweites juristisches Staatsexamen
Januar 2014 – September 2015	Tätigkeit als angestellte Rechtsanwältin in der Rechtsanwaltskanzlei Klaus Ohnesorge in Emmelshausen (2,5 Tage / Woche)
Seit September 2015	Tätigkeit als Syndikusrechtsanwältin und Bereichsleiterin (Justiziariat, Grundstücksangelegenheiten, Ausschreibungen) bei der Stadtwerke Neuwied GmbH in Neuwied